Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Аналіз інформаційної безпеки телекомунікаційної мережі з хмарною технологією
(тема)

Виконав:
студент 2 курсу, групи АМСЗІм-18-1
Скирда С.О.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: проф. кафедри ІКІ ім. В.В. Поповського
Марчук В.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2020р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студенту Скирді Станіславу Олеговичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Аналіз інформаційної безпеки телекомунікаційної мережі з хмарною технологією
затверджена наказом по університету від «17» березня 2020р. № 465 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 10.05.2020р.
3. Вихідні дані до роботи: огляд типів телекомунікаційних мереж з хмарною технологією, аналіз методів проведення аудиту інформаційної безпеки, методи проведення експертного аудиту інформаційної безпеки на основі використання штучної нейронної мережі, дослідження методів захисту мереж з хмарними технологіями по результатам аудиту.
4. Перелік питань, що потрібно опрацювати в роботі:
1) Проведення аудиту ІБ з точки зору системного аналізу
2) Розробка методу та структурної схеми, що реалізує метод проведення експертного аудиту інформаційної безпеки в системі хмарних обчислень
3) Дослідження методів захисту мереж з хмарними технологіями по результатам аудиту
4) Необхідно провести аудит системи з хмарною технологією. Схема системи, що підлягає аудиту наведена в додатку А

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій:
Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	професор Марчук Володимир Степанович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	17.02.2020	Виконано
2	Збір матеріалів для дослідження	01.03.2020	Виконано
3	Розробка 1 розділу	25.03.2020	Виконано
4	Розробка 2 розділу	08.04.2020	Виконано
5	Розробка 3 розділу	25.04.2020	Виконано
6	Розробка 4 розділу	01.05.2020	Виконано
7	Оформлення атестаційної роботи	10.05.2020	Виконано

Дата видачі завдання 17 лютого 2020 року

Студент _____ Скирда С.О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ професор Марчук В.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 29 рис., 2 табл., 3 додатки, 22 джерела.

ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ, ХМАРНІ ТЕХНОЛОГІЇ, АУДИТ, ЗАХИСТ ІНФОРМАЦІЇ, ПРАВА ДОСТУПУ, БЕЗПЕКА, ЗАГРОЗИ, VPN.

Об’єкт дослідження – процес проведення аудиту інформаційної безпеки телекомунікаційних мереж з хмарною технологією.

Предмет дослідження – методи і засоби проведення аудиту інформаційної безпеки телекомунікаційних мереж з хмарною технологією.

Мета роботи – аналіз методів проведення експертного аудиту інформаційної безпеки телекомунікаційних мереж з хмарною технологією.

Методи дослідження – аналіз, синтез та порівняння.

У роботі розглядається аудит інформаційної безпеки телекомунікаційних мереж з хмарною технологією на основі використання штучної нейронної мережі.

На основі отриманих даних аудиту досліджені методи захисту мереж з хмарними технологіями.

ABSTRACT

Explanatory note: 73 p., 29 fig., 2 tables, 3 application, 22 sources.

TELECOMMUNICATIONS NETWORKS, CLOUD TECHNOLOGIES, AUDIT, INFORMATION PROTECTION, ACCESS RIGHTS, SECURITY, THREATS, VPN.

The object of research is the process of information security audit of telecommunication networks with cloud technology.

The subject of research – methods and means of conducting information security audits of telecommunications networks with cloud technology.

The purpose of the work is to analyze the method of conducting an expert audit of information security of telecommunication networks with cloud technology.

Research methods – analysis, synthesis and comparison.

The paper considers the information security audit of telecommunication networks with cloud technology based on the use of an artificial neural network.

On the basis of the received audit data methods of protection of networks with cloud technologies are investigated.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АС – автоматизована система
ІБ – інформаційна безпека
ІС – інформаційна система
ІТ – інформаційні технології
ОС – операційні системи
ПІБ – підсистема інформаційної безпеки
ПЗ – програмне забезпечення
ПК – персональний комп'ютер
СЗІБ – система забезпечення інформаційної безпеки
СУБД – система управління базами данних
ЦОД – центр обробки даних
ШНМ – штучна нейронна мережа
ALE – annual loss expectancy
CA – certification authority
CIS – center for internet security
DHCP – dynamic host configuration protocol
IaaS – infrastructure as a service
IDS – intrusion detection system
IP – internet protocol
IPS – image packaging system
ITSEC – information technology security evaluation criteria
NAT – network address translation
PaaS – platformas as service
ROI – return on investment
SaaS – software as a service
SAN – storage area network
SCORE – security consensus operational readiness evaluation
SSL – secure sockets layer
TCP – transmission control protocol
VPN – virtual private network

ВСТУП

В наш час спостерігається значне зростання попиту на інформаційні послуги. Інформаційне забезпечення впроваджується в усі сфери людської діяльності. Але разом з тим зростає і кількість небезпек для інформації, що передається. Дані є найбільш важливим компонентом інформації. Роль інформації у житті людей зростає. Загрози втрати і викрадення даних збільшуються. Томузростає необхідність їх захисту. При чому кількість інформаційних потоків збільшується, і саме через це важко зорієнтуватися та виявити загрозу на ранніх стадіях, а особливо важко попередити її.

Організаціям і фірмам необхідно впроваджувати різні ефективні заходи захисту незалежно від видів бізнесу чи форми власності для успішного функціонування таких систем.

Будь-яка організація – це сукупність взаємодіючих підрозділів, кожен з яких може мати свою структуру. Вони пов'язані між собою функціонально, тобто виконують окремі види робіт у рамках єдиного бізнес-процесу, а також інформаційно, обмінюючись документами, факсами, письмовими та усними розпорядженнями та ін. Крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційною, так і функціональною. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вони не займалися – для урядової установи, банку, промислового підприємства, комерційної фірми та ін.

Розподіленість по території окремих елементів фірми потребує територіально розподілених телекомунікаційних технологій. Одна з таких технологій – це хмарна технологія.

Телекомунікаційна мережа з хмарною технологією, як правило, є територіально розподіленою, тобто об'єднує офіси, підрозділи та інші структури, що знаходяться на значній відстані один від одного. Принципи, за якими будується телекомунікаційна мережа з хмарною технологією, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні телекомунікаційної мережі з хмарною технологією слід вживати всіх заходів для мінімізації обсягів переданих даних. В іншому ж телекомунікаційна мережа з хмарною технологією не повинна

вносити обмежень на те, які саме додатки і яким чином обробляють загальну інформацію [1].

Використання сторонніх платформ, що надають хмарні послуги,також потребує особливої уваги до забезпечення бепеки систем зв’язку.

Тому для всебічного аналізу телекомунікаційних мереж з хмарною технологією та її компонентів, виявлення «вузьких» місць, що роблять мережну інфраструктуру вразливою і небезпечною з точки зору конфіденційності корпоративних даних, використовується мережний аудит.

Аудит мережі з хмарною технологією – це дослідження поточного стану, конфігурації, працездатності і відмовостійкості телекомунікаційної мережі з хмарною технологією.

Мережний аудит є необхідним, коли відзначаються проблеми в роботі мережі, передачі сигналу або збій при наданні сервісів, а також перед початком робіт з модернізації мережі і після завершення для оцінки результатів модернізації.

Окрім цього аудит мережі широко використовують для оцінки якості послуг, що надаються Інтернет-провайдерами або при передачі мереженої інфраструктури на аутсорсинг.

До того ж, аудит мережі носить велику цінність для бізнесу, адже допомагає зберегти безпеку корпоративних даних, забезпечити ефективність та відмовостійкість мережі, знизити ризики надання онлайн сервісів клієнтам по неякісних каналах [2].

Враховуючи все вище вказане, можна зробити висновок, що проведення аудиту інформаційної безпеки є досить актуальним питанням, саме тому темою даної атестаційної роботи є дослідження аудиту телекомунікаційних мереж з хмарною технологією, як однієї із ключових складових інформаційної системи. Окремі результати роботи доповідались на XXIV Міжнародному молодіжному форумі «Радіоелектроніка та молодь у XXI столітті» [3].

1 ЗАХИСТ ІНФОРМАЦІЇ В ХМАРНИХ ТЕХНОЛОГІЯХ

1.1 Загальні методи забезпечення інформаційної безпеки

В представленій роботі розглянуті етапи зберігання, обробки і передачі інформації незалежно від виду її кодування, від виду об'єкта або, безпосередньо, від самої смислового навантаження. Через це коло використання терміна «інформаційна безпека» значно звужується.

У нашому випадку, під «інформаційною безпекою» ми будемо розуміти ступінь захисту інформації, що забезпечує існування інфраструктури від небажаного (випадкового або спеціального) впливу, яке здатне завдати збитку учасникам інформаційних відносин.

Захист інформації складається з набору заходів безпеки. Для виявлення проблем інформаційної безпеки, спочатку необхідно визначити учасників даних відносин і їх інтересів, дотичних до використання інформаційних систем. Загрози інформаційної безпеки це невід'ємна частина, що виникає завжди при використанні інформаційних технологій. Можна зробити два важливих висновки.

1) Відповідно до відмінності категорій суб'єктів в інформаційних відносинах, проблеми, що виникають в процесі організації захисту, істотно відрізняються. Цю ситуацію можна розглянути на прикладі державної організації і навчального закладу. Для першого суб'єкта краще знищити всі дані, ніж допустити ймовірність їх витоку. У другому навпаки - головне щоб все працювало, ніяких секретів не зберігають.

2) В задачах інформаційної безпеки варто забезпечити не тільки захист, з метою запобігання від несанкціонованого доступу до інформації, а і якість функціювання систем зв’язку. Учасники інформаційних відносин можуть понести збитки ще й від проблем, пов'язаних з функціонуванням системи, яка веде до збоїв в роботі. Для таких організацій, як навчальні заклади, захист стоїть не на першому місці.

3) Варто відмітити, що під терміном «комп'ютерна безпека» мається на увазі не тільки процес обробки і зберігання даних, на комп'ютерах. Комп'ютер є лише частиною в ланцюжці інформаційні системи. Тому інформаційна безпека також залежить від підтримуючої інфраструктури [4].

Неможливо передбачити і запобігти всім загрозам безпеки інформації. В трактуванні терміна «інформаційна безпека» присутнє словосполучення «неприйнятний збиток». Заходи щодо забезпечення безпеки можуть виявитися затратними з економічної точки зору. Тому, будь-які можливі ризики потрібно адекватно оцінювати і зіставляти з витратами по їх запобіганню. Але є ряд загроз, таких як, можливий збиток стану здоров'я людини або навколишнього середовища, які відносяться до категорії неприпустимих загроз. Тому в їх відношенні необхідно застосовувати всі заходи щодо запобігання.

Існує два основних типи загроз інформаційній безпеці: штучні та природні. Види штучних загроз інформаційних систем зображені на рис. 1.1.

Рисунок 1.1 – Види штучних загроз інформаційної системи

Ненавмисними загрозами вважаються дії, вчинені людьми через відсутність належної уваги, необхідної обережності, достатніх знань.

До прикладів ненавмисного типу загроз можна віднести зайву установку програмного забезпечення, яке не є необхідним для роботи. Надалі ці надлишкові продукти можуть стати причиною збою в роботі. Так само можна привести в приклад таку людську особливість, як цікавість. Вчинені дії через незнання не є злим умислом, але можуть стати причиною збитку. Такий тип загроз складно передбачити та проконтролювати [5].

Навмисними загрозами вважаються загрози, навмисно спрямовані на фізичне руйнування з подальшим виходом системи з ладу.

До прикладів такого типу загроз можна віднести атаки на інформаційну систему внутрішнього і зовнішнього характеру. Найчастіше внутрішньому захисту інформаційної системи приділяють значно менше уваги, ніж зовнішньому захисту. Відомі випадки багатомільйонних втрат у великих компаніях через внутрішній злом системи та крадіжку даних.

Штучні загрози можна розбити на категорії.

1) Дії користувачів, які авторизувалися в системі.

2) Вплив «електронного» характеру.

Під цим розуміються дії хакерів з цілеспрямованим зломом системи для отримання вигоди, або просто з цікавості. Прикладом є несанкціонований доступ до даних, метою якого є проникнення в корпоративну мережу підприємства ззовні. При отриманні доступу до даних хакери використовують його для нанесення шкоди. Використовуючи мережеву інфраструктуру, хакери можуть здійснювати атаки не тільки на вузли підприємства, а й на вузли третіх фірм, конфіденційна інформація про яких зберігається на атакованому підприємстві.

Інша загроза це - комп'ютерні віруси. Для сучасного ведення бізнесу комп'ютерні віруси є серйозною загрозою. На даний момент практично будь-яка компанія має свою інформаційну систему та активно її використовує в роботі. Зараження корпоративної мережі комп'ютерними вірусами може привести до відмови роботи всіх інформаційних сервісів, перебоїв в роботі, розкрадання даних або їх знищення. Проникнення вірусних програм в мережу підприємства може дати зловмисником повний або частковий контроль над всіма операціями компанії.

Ще одна загроза це спам. Темпи зростання впливу загрози спаму з кожним роком все більше. Спам навантажує надлишковою та непотрібною інформацією, яка може виявитися шкідливою. Великим каналом для розповсюдження спаму є електронна пошта.

З природними загрозами ситуація куди-більш очевидна. До даного типу загроз відноситься крадіжка фізичного обладнання з інформацією, наприклад, комп'ютера або різних носіїв. Так само до них відносяться всі види стихійних лих: цунамі, урагани, удари блискавок, пожежі.

Загроза пожежі трапляється найчастіше. У даній ситуації, заходи щодо забезпечення пожежної безпеки відносяться не тільки до забезпечення безпеки життя людей, а й безпеки інформації. Зважаючи на все вище сказане можна скласти структуру методів забезпечення інформаційної безпеки. Структура зображена на рис. 1.2.

Рисунок 1.2 – Методи забезпечення інформаційної безпеки

Правові способи по забезпеченню безпеки охоплюють розробку нормативно-правових актів, що регламентують інформаційні відносини між учасниками, і нормативно-методичних документів, що показують питання забезпечення інформаційної безпеки [6].

Актуальними в сфері безпеки вважаються:

- своєчасне внесення змін і доповнень, що стосуються регулювання відносин у сфері безпеки інформації, в законодавство держави;
- знищення розбіжностей, пов'язаних з інтернаціональними угодами;
- встановлення відповідальності за правопорушення;
- розмежування можливостей в області забезпечення інформаційної безпеки;
- розробка та прийняття нормативних правових актів;
- організаційно - технічні заходи;
- створення та модернізація системи по забезпеченню інформаційної безпеки;
- розробка, впровадження та поліпшення засобів захисту інформації та способів контролю продуктивності даних засобів;
- виявлення технічних приладів і програм, що становлять загрозу для безпеки інформації;
- сертифікація засобів захисту інформації;
- контроль за діями персоналу в захищених інформаційних системах;
- складання системи прогнозу характеристик інформаційної безпеки.

Фінансові заходи з надання безпеки містять:

- розробку намірів щодо забезпечення інформаційної безпеки;

- поліпшення системи фінансування справ, пов'язаних з організацією правових та організаційно-технічних заходів.

1.2 Поняття та характеристика хмарних обчислень

Cloud computing, що в перекладі з англійської означає – хмарні обчислення. Cloud computing – технологія надання користувачу можливості використання віддалених ресурсів і потужностей. Обчислення відбувається за принципом розподіленої обробки даних. Її суть полягає в забезпеченні користувача віддаленим доступом до наданих в хмарі послуг. Потреба в економії коштів за рахунок ефективних заходів з надання послуг у сфері хостингу вплинула на розвиток цієї технології [7].

Під терміном «хмарні обчислення» сьогодні розуміють набір різних сервісів, доступ до яких здійснюється через мережу Інтернет. Хмарні технології є потужним рішення, пов'язаних з рішенням ресурсомістких завдань. Популярність їх використання весь час зростає. Всі користувачі персональних комп'ютерів або зверталися до послуг хмарних сервісів, або вже активно їх використовують.

Поняття хмарних обчислень має широкий спектр застосування. Тому має сенс його логічного поділу на кілька груп. На рис. 1.3 можемо бачити архітектуру хмарних сервісів.

Рисунок 1.3 – Архітектура хмарних сервісів

SaaS – послуга хмарних додатків, ймовірно, найбільш популярна і проста форма у використанні хмарних обчислень. SaaS використовує мережу Інтернет для достаки додатків, які управляються сторонніми постачальниками та чий

інтерфейс доступний клієнтській стороні. Більшість SaaS додатків можна запускати безпосередньо з веб-браузера, без необхідності завантаження або попередньої установки. SaaS позбавляє від необхідності встановлювати та запускати додатки на персональних комп'ютерах. З використанням SaaS, спрощується задача підприємств по раціональному технічному обслуговуванні і підтримці. В послуги постачальника входить обслуговування: додатків, часу виконання, даних, проміжного програмного забезпечення, операційних систем, віртуалізації серверів, сховищ і мереж. Gmail є одним відомим прикладом поштового оператора SaaS [5].

PaaS – найскладніший з трьох видів – хмарна платформа послуг, що розподіляє обчислювальними ресурсами через окрему платформу. Розробники отримують з PaaS можливість, де вони можуть створити свої додатки або виконати налаштування додатків. PaaS робить розробку, тестування і розгортання додатків швидким, простішим та економічно ефективним, позбавляючи користувача від необхідності купувати нижні шари апаратного і програмного забезпечення. Одна відмінність між SaaS і PaaS пов'язан з тим, що деякі аспекти в PaaS управляються користувачами, а не постачальниками.

PaaS надає обчислювальні інфраструктури, обладнання і платформи, які встановлені на верхній частині апаратного забезпечення. Подібно до того, як можна створювати макроси в Excel, PaaS дозволяє створювати додатки, використовуючи програмні компоненти, які управляються за допомогою стороннього постачальника. PaaS добре масштабується і користувачам не доведеться турбуватися про оновлення платформи або їх сайт вийде з ладу під час технічного обслуговування. Користувачі, які отримують найбільшу віддачу від PaaS, це компанії, які бажають підвищити ефективність і інтерактивність великого штату співробітників [5].

IaaS – хмарна інфраструктура послуг, що поставляє комп'ютерну інфраструктуру (наприклад, платформу віртуалізації середовища), сховище і мережу. Замість того, щоб купувати програмне забезпечення, сервера або мережеве обладнання, користувач може купити все це як повністю зовнішній сервіс, рахунок за який зазвичай залежить від кількості ресурсів, що споживаються. Іншими словами, третя сторона за орендну плату дозволяє користувачу встановити віртуальний сервер на їх IT-інфраструктурі. У порівнянні з SaaS і PaaS, IaaS користувачі несуть велику відповідальність за управління:

додатками, даними, часом виконання, проміжним ПЗ та операційними системами. Постачальники послуги як і раніше контролюють віртуалізацію, сервера, жорсткі диски, сховища і мережу. Користувачі IaaS отримують можливість повного доступу до готової інформаційної інфраструктури, в середині якої вони можуть встановити необхідні платформи. Користувачі несуть відповідальність за оновлення, якщо нові версії платформ вийшли з ладу.

Існує ще один поділ хмар на публічні та приватні. Послуги, що надаються публічними хмарами, можуть бути доступні будь-якому користувачеві. Яскравим прикладом публічної хмари є Amazon Web Services. Головна різниця між публічними та приватними хмарами в тому, що до останніх здійснюється закритий доступ тільки для обмеженого числа користувачів.

1.3 Плюси та мінуси використання хмарних технологій

До переваг хмарних технологій можна віднести.

1) Порівняно дешеві комп'ютери для користувачів. Пропадає необхідність купувати комп'ютери високої потужності з великим об'ємом пам'яті та дисків, тому, що вся інформація і всі програми зберігаються на серверах в «хмарі» і запускаються віддалено. З великих стаціонарних персональних комп'ютерів і звичайних ноутбуків користувачі можуть перейти на компактні нетбуки.

2) Зростає продуктивність комп'ютерів для користувачів. За рахунок віддаленого запуску файлів і програм, комп'ютери користувачів не обтяжені цією роботою і функціонують швидше. Як приклад, можна розглянути роботу Panda Cloud Antivirus - програма антивірус, доступна як Веб сервер. Panda Cloud Antivirus надає можливість сканувати дані на віруси віддалено на потужних серверах. Запуск цієї ж програми безпосередньо на самому комп'ютері користувача за допомогою його власних ресурсів збільшувало б навантаження приблизно у 2 рази.

3) Підвищується ефективність використання IT інфраструктури і йде зниження витрат. Якщо взяти середню оцінку завантаження сервера для компанії, то вона складе близько 13%. Іноді для компанії з'являється необхідність використовувати додаткові потужності, але більшість часу обчислювальні ресурси нічим не зайняті. Якщо ж використовувати обчислювальні ресурси на

віддалених серверах в «хмарі», то витрати компанії по цій частині можуть скоротитися вдвічі. З урахуванням мінливої економічної обстановки гнучкість виробництва зростає. Компанії, які не довіряють збереження своїх даних стороннім організаціям, мають можливість побудувати свою власну хмара та отримувати всі переваги від віртуалізації інфраструктури.

4) Зниження витрат на обслуговування і закупку ПЗ. З використанням технології Cloud Computing власних серверів у компаній стає менше, тому обслуговувати їх стає легше. Зі зменшенням кількості фізичних серверів проблеми з придбанням програмного забезпечення також зменшуються. Через те, що сервіси та додатки знаходяться в «хмарі», нема потреби купувати ПЗ для кожного користувача. Компанія купує потрібні програми в «хмарі». Вартість сервісів, пропонованих з доступом через Інтернет, на порядок нижче аналогів, які існують для персональних комп'ютерів. Більш того, є можливість погодинної оренди використання програм, а витрати на підтримку ПЗ в робочому стані і його оновлення дорівнюють нулю.

5) Зростання обчислювальної потужності. У порівнянні з персональним комп'ютером, обчислювальні ресурси хмари надають величезні можливості. Обчислювальна потужність хмари визначається кількістю його серверів. Інакше кажучи, користувачам надається віддалений доступ до суперкомп'ютера, який дає можливість вирішувати більш складні та об'ємні завдання, непосильні звичайному ПК.

6) Необмежений обсяг для зберігання даних. Обсяг наданого місця в хмарі для зберігання даних може гнучко та автоматично підлаштовуватися, в залежності від побажань користувача. Якщо для користувача персональним комп'ютером звичайна ситуація – це нестача місця для даних, то для користувача хмарних обчислень це практично неможливо.

7) Сумісність з операційними системами. Для хмарних технологій неважливо, яка операційна система стоїть у користувача. Клієнт з системою Microsoft Windows може без проблем обмінюватися даними через хмару з користувачами системи Unix. Що стосується доступу до сервісів хмарних обчислень, то вони надаються за допомогою стандартних для кожної операційної системи браузерів.

8) Сумісність форматів документів. У хмарних обчислень відсутнє поняття несумісності форматів документів, створених в різних версіях однієї хмарної програми.

9) Легкість спільної роботи для групи користувачів. В системі хмарних обчислень з'являється зручна можливість одночасної роботи декількох учасників. Немає потреби займатися перенесенням документів з комп'ютера на комп'ютер. Редагування документів відбивається миттєво, причому користувачеві завжди доступна остання версія оновленого документа.

10) Повсюдний доступ до файлів користувача є великою перевагою використання хмарних обчислень. Якщо дані зберігаються в хмарі, вони завжди доступні для їхнього власника при наявності доступу в мережу Інтернет. Також перед користувачем відкривається широкий вибір різних пристроїв, з яких він може здійснити цей доступ. Клієнт хмари може скористатися персональним комп'ютером, нетбуком, ноутбуком, планшетним комп'ютером, смартфоном.

11) Зменшення використання природних ресурсів. З технологією хмарних обчислень економія йде не тільки на електроенергії, обчислювальних потужностях і фізичному просторі, а й і на ресурсах природи. Центри обробки даних можна розташовувати вже свідомо в холодному кліматі. Устаткування для доступу до даних тепер компактніше, вимагає для виготовлення менше матеріалів.

12) Стійкість даних до втрати. Дані, що зберігаються в хмарі, розподіляють свої копії по декількох серверах. Імовірність втрати даних в хмарі куди менше ймовірності їх втрати при зберіганні на звичайних фізичних носіях інформації.

До недоліків хмарних технологій можна віднести.

1) Постійна необхідність з'єднання з мережею Інтернет. Для технології хмарних обчислень завжди необхідно з'єднання з мережею Інтернет. Існує, звичайно, ряд додатків, які завантажуються на комп'ютер і дозволяють подальшу роботу не дивлячись на з'єднання. В інших випадках все просто: немає з'єднання – немає роботи. На думку багатьох, це найбільший недолік хмарних обчислень. Але якщо врахувати розвиток інформаційних технологій в наш час, то можна з упевненістю сказати, що доступ в мережу Інтернет є практично скрізь. Тому незабаром така проблема і зовсім зникне.

2) Погано працює з повільним з'єднанням. Більшість хмарних сервісів вимагають для нормальної роботи швидке Інтернет-з'єднання. Але як говорилося вище, інформаційні технології не стоять на місці, тому зараз немає проблем з пропускною спроможністю з'єднань мережі Інтернет.

3) Програми можуть працювати повільно і з неповними функціональними можливостями. Деякі з програм, що надаються хмарними послугами, працюють на локальному комп'ютері швидше. Це може бути пов'язано як з невисокою пропускною здатністю з'єднання мережі Інтернет, так і завантаженістю віддалених серверів. Також, програми, представлені в хмарі, мають обмежений функціонал, на відміну від їх версій для локального комп'ютера.

4) Існує загроза безпеки даних. Безумовно, якщо ви передаєте дані в хмару, то відразу виникає можливість загрози безпеки інформації. Але тут вся справа полягає в довірі до провайдера. Якщо постачальник хмарної технології надійно шифрує передачу інформації, створює резервні копії та вже має великий досвід на ринку в даній сфері, то порушення системи безпеки може ніколи не трапитися.

5) Факт, що втрата даних в хмарі є безповоротною. Але довести до такого стану куди складніше, ніж втратити їх на локальному комп'ютері.

6) Не дивлячись на безліч переваг над недоліками, в кожній ситуації все відбувається по-різному. Кожен сам оцінює всі критерії та приймає вибір: використовувати хмарні обчислення чи ні [6].

1.4 Проблеми захисту хмарних обчислень

Протягом останнього часу постійно піднімається питання про перспективу розвитку хмарних обчислень. Це пов'язано з колосальним приростом бізнесу і інформаційної інфраструктури. Основна суть технології хмари полягає в наданні різних інформаційних платформ та додатків для користувача через мережу Інтернет. Головна ідея – це звільнення ресурсів персонального комп'ютера користувача, і перенесення цього навантаження на віддалені обчислювальні потужності. Гігантські обчислювальні потужності, що знаходяться віддалено, надають можливість мати практично необмежений об’єм сховища для зберігання даних, величезну обчислювальну продуктивність і миттєвий доступ до даних

будь-якому користувачу-клієнту за кошти інтернет з'єднання. Аналогічно, є можливість для компаній створювати власні хмари, де співробітники користуються всіма привілеями даної технології, співробітнику потрібно лише мати доступ до корпоративної мережі.

Йде інтенсивна рекламна компанія, що представляє хмарні технології, тому вирішення проблеми інформаційної безпеки відкладаються на пізній час, ставлячи під загрозу не тільки дані користувачів, але і стійкість всієї структури в цілому. А це може привести до великих втрат прибутку і інших втрат.

Основні принципи щодо забезпечення безпеки інформації в комп'ютерних системах, які вдалося розробити за останні 20 років, можна використовувати і в хмарних обчисленнях. У статті [7] розкриті невирішені проблеми інформаційної безпеки хмарних обчислень.

Для аналізу взята організація «хмарних» обчислень на основі центру обробки даних (ЦОД), що реалізує принцип віртуалізації обчислень. Система обчислень в «хмарі» ділиться на шість основних частин.

1) Апаратні компоненти центру обробки даних.
2) Телекомунікаційна складова доступу до ресурсів центру обробки даних.
3) Учасники та їх програмно-апаратне забезпечення.
4) «Середній» (middleware) шар центру обробки даних.
5) Прикладні сервіси.
6) Системи зберігання даних (СЗБД).

1.5 Існуючі види хмарних послуг і моделей хмарного розміщення

Сучасні тенденції розвитку IT-індустрії дозволяють переходити від традиційних методів обробки інформації до більш прогресивних. Одним з таких методів є перенесення обчислень організації - споживача в хмарні структури провайдера хмарних обчислень, що є постачальником хмарних послуг. Обчислення в хмарі базуються на сукупності різних технологій. Хмарні обчислення дозволяють не ускладнювати інформаційну інфраструктуру споживача хмарних послуг завдяки використанню об'єднаних в віртуальну інфраструктуру ресурсів постачальника.

Хмарна інформаційна система складається з хмарного клієнта і хмарного сервера. Під хмарним клієнтом розуміються кошти обчислювальної техніки, що входять до складу інформаційної системи, побудованої з використанням технологій хмарних обчислень, за допомогою яких здійснюється отримання однієї або декількох хмарних послуг.

Хмарний сервер – розподілена обчислювальна мережа для обробки запитів споживачів хмарних послуг. Хмарний сервер може мати в своєму складі мережеве обладнання, сервери обробки даних, операційну систему (ОС), мережеві сховища, засоби управління базами даних, прикладні програми, мережеві служби і ін.

На віртуальному сервері, що знаходиться в «хмарі» постачальника, під керуванням різних операційних систем може одночасно функціонувати безліч додатків споживачів хмарних послуг. Віртуальний поділ ресурсів дозволяє створювати мережеві домени, що надають послуги різним споживачам по обробці конфіденційної інформації.

При використанні моделі доступу «хмарні обчислення», інформаційні сервіси надаються таким чином, що технології забезпечення стають практично «невидимими» для споживача. А оскільки це дозволяє відокремити інформаційні сервіси від технологій забезпечення, то бізнес може швидше адаптуватися до змін.

Поява першої технології, близькою до сучасного розуміння терміна «cloud computing», приписується компанії Salesforce.com, заснованої в 1999 році [8]. Саме тоді і з'явилося перше речення нового виду – «Програмне забезпечення як сервіс» ("Software as a Service" або "SaaS"). Перше бізнес-рішення під назвою «Amazon Web Services» було запущено в 2005 році компанією Amazon.com, яка активно займалася модернізацією своїх центрів обробки даних (ЦОД). Найбільш характерний приклад додатків хмарних обчислень, що сьогодні широко використовуються – це служба Google Docs, яка дозволяє працювати з офісними документами через браузер споживача. У табл. 1.1 показані етапи розвитку ринку хмарних обчислень починаючи з 2007 року.

Таблиця 1.1 – Етапи розвитку ринку хмарних обчислень

Етап	Період часу	Особливості
Час першого етапу використання	2007-2010 р.	Хмарні обчислення впроваджують ті компанії, які готові йти на ризики.

Продовження таблиці 1.1

Етап	Період часу	Особливості
Консолідація ринку	2010-2012 р	Консервативні користувачі починають звертати увагу на хмарні обчислення; росте конкуренція і знижується загальна кількість постачальників.
Масове поширення	Після 2012 р.	Хмарні обчислення стають переважаючим напрямком в розвитку IT індустрії.

Сам факт високої зацікавленості найбільших гравців ринку IT демонструє певний статус хмарних обчислень як найбільш привабливого напрямку для розвитку IT-індустрії. У квітні 2014 року аналітична компанія Forrester Research опублікувала прогноз розвитку ринку публічних хмарних обчислень до 2020 року. Графік зображено на рис. 1.4. Згідно з відомостями звіту, до 2020 р. обсяг хмарного ринку склав $ 160 млрд [9].

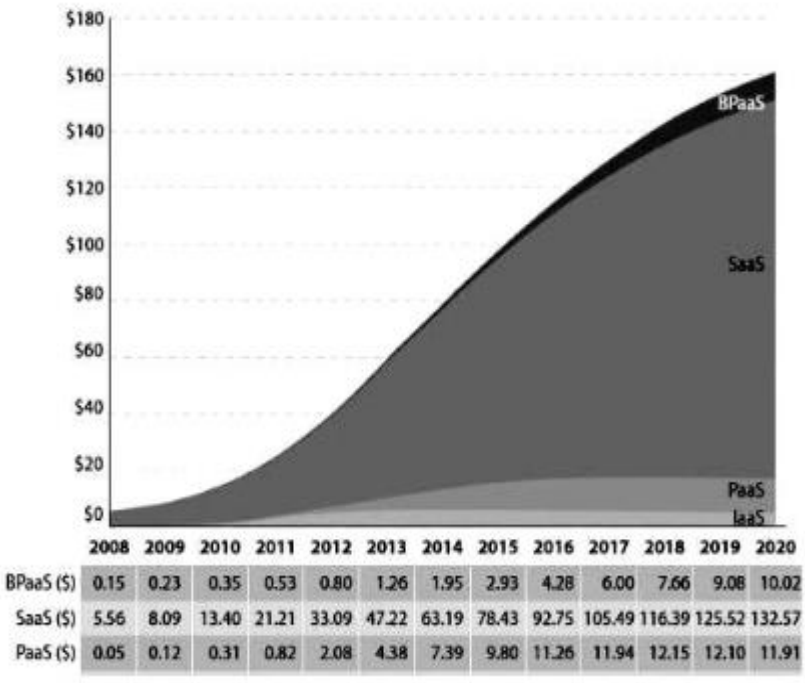

Рисунок 1.4 – Динаміка розвитку ринку хмарних обчислень

З аналізу наведеного графіка видно, що розвиток хмарних технологій продовжується і ще не досяг свого піку.

Існує безліч видів хмарних послуг і моделей хмарного розміщення. Компаніям споживачам хмарних послуг необхідно зрозуміти різницю між наявними типами хмарних середовищ і визначити, які з них найкращим чином відповідають їх бізнес-процесам.

Розрізняють декілька моделей хмарного розміщення. Приватна хмара (private cloud) – інфраструктура, призначена для використання однією організацією, що включає кілька споживачів (наприклад, підрозділів однієї організації), а також можливо для клієнтів та підрядників даної організації. Приватна хмара може перебувати у власності, управлінні та експлуатації як самої організації, так і третьої сторони (або будь-якої їх комбінації), і може фізично існувати як в середині, так і поза юрисдикцією власника.

При використанні приватної хмари знижується час очікування надання ресурсів для співробітників компанії споживача хмарних послуг. Хмарне середовище сприяє ефективному розподілу ресурсів в середині організації, допомагає динамічно розподілити навантаження між фізичними системами ЦОД. З'являється можливість відстежувати реальне споживання ресурсів в середині компанії.

Наступним варіантом розгортання є публічна хмара – це хмарна система, підготовлена постачальником хмарних послуг для відкритого використання декількома компаніями. Хмара існує тільки на території хмарного постачальника, на відміну від приватної хмари.

Змішана хмара – це спільне використання двох перерахованих вище моделей розгортання. Така модель являє собою композицію з двох або більше різних інфраструктур хмар, що мають унікальні об'єкти, але пов'язаних між собою стандартизованими або власними технологіями, які дозволяють переносити дані або програми між компонентами. Концепція гібридних хмар зображена на рис. 1.5.

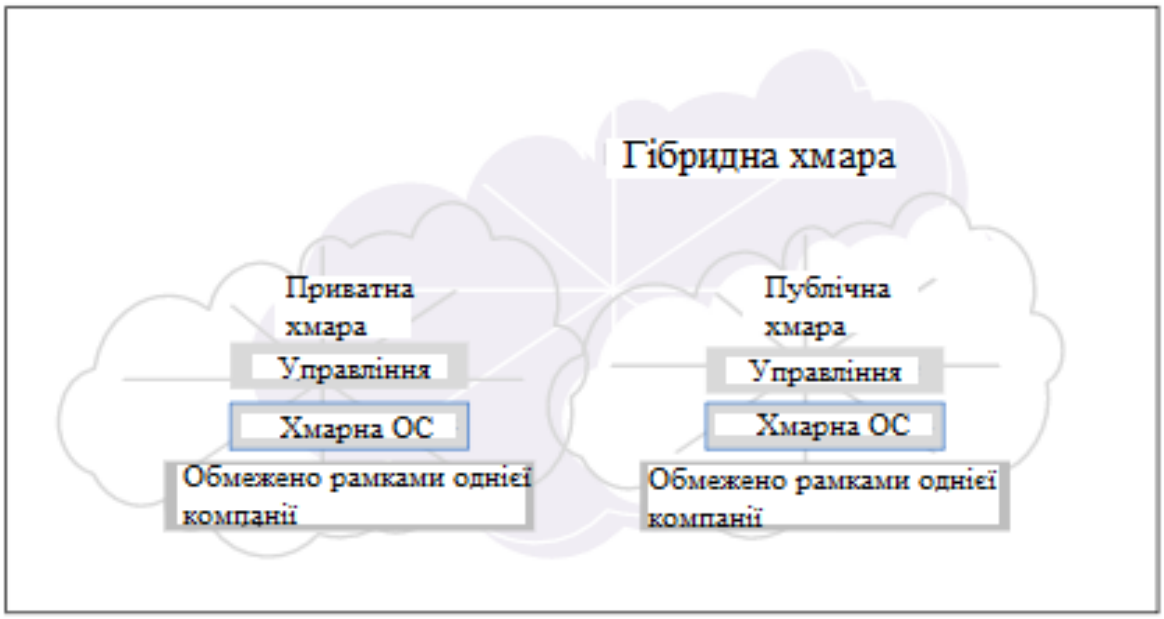

Рисунок 1.5 – Концепція гібридної хмари

Використання технологій приватної, публічної і гібридної хмари дозволяють користувачам хмарних обчислень скористатися обчислювальними потужностями та сховищами даних, які за допомогою певних технологій віртуалізації та високого рівня абстракції надаються їм як послуги. Розглянемо сучасні види хмарних послуг, самі популярні з них проілюстровані на рис. 1.6.

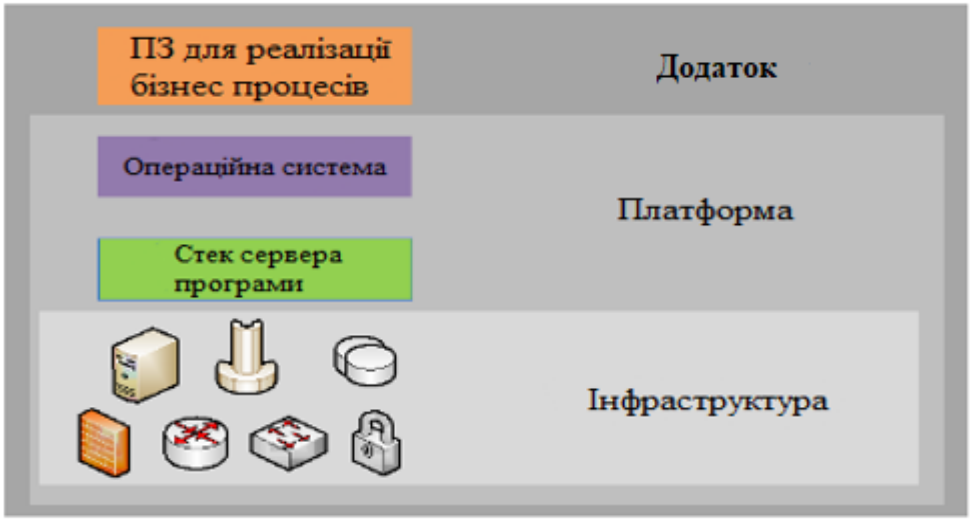

Рисунок 1.6 – Сучасні види хмарних послуг

Найнижчий рівень і найбільш проста модель розгортання хмарних сервісів дозволяє замовнику взяти в оренду тільки інфраструктуру, яка називається IaaS.

Більш складна модель розгортання хмарних обчислень охоплює рівень платформи інформаційної системи та отримала назву PaaS. Цей рівень містить не тільки інфраструктуру, але і деякі сервісні служби, наприклад операційні системи і їх обслуговування.

Модель розгортання хмарних сервісів, що характеризується найбільш повним наданням послуг замовникові, передбачає використання додатків із хмари для роботи на локальному комп'ютері замовника і називається SaaS. Багато SaaS рішень є заміною традиційного програмного забезпечення і формою перенесення його в хмарне середовище. Сучасні SaaS рішення та їх аналоги відображені в табл. 1.2.

Таблиця 1.2 – Сучасні SaaS-рішення та їх аналоги

Традиційне ПЗ	Хмарне ПЗ
MS Outlook	Gmail, Office 365
Dynamics CRM/Oracle CRM	Saleaforce.com
1С	Ельба, Моє діло, Мій склад
MS Project	Мегаплан, Basecamp
Microsoft Office	Google Apps, Office 365

Таким чином, для споживача хмарних послуг відкриваються широкі можливості, що дозволяють знизити вимоги до обчислювальної потужності власної інформаційної системи, а будь-якому слабкому обчислювальному пристрою отримати потенціал найсучаснішого і дорогого устаткування.

Розглянемо приклад архітектури ICOT, що реалізується компанією IBM. З точки зору апаратної частини хмара являє собою центр IBM BladeCenter H з необхідною кількістю серверів HS22 на основі Intel архітектури. До вбудованого в центр SAN комутатора підключається зовнішня система зберігання даних DS5020, що є хмарним сховищем даних. Один сервер виділений під управління хмарою, в нього не рекомендується ставити віртуальні машини в цілях безпеки. Два інших використовуються під менш критичні засоби управління хмарним середовищем. На решту встановлюються віртуальні машини по одному додатку та гостьовими операційними системами. Як гіпервізор в даній архітектурі використовується VMware ESX. Керуючі компоненти гіпервізору розділені на дві частини. Перші працюють під управлінням Windows 2003 з тієї причини, що

VMware Virtual Center не підтримує інші платформи. Ці компоненти можна поставити у віртуальне середовище, тому що вони не є її частиною, а служать надбудовою. Вони керують віртуальним середовищем. Virtual Center дозволяє швидко діагностувати проблеми з віртуальної інфраструктури. Systems Director управляє апаратної платформою і за допомогою модуля VM Control забезпечує надійність віртуального середовища в разі апаратних збоїв. Більшість компонентів хмари знаходиться на зовнішній системі зберігання даних. Це пов'язано с тим, що дані повинні бути доступні з декількох серверів одночасно. Друга група керуючих компонентів працює під управлінням гіпервізора і надає базові хмарні сервіси, такі як управління сервісами, управління образами програмного забезпечення, розгортання нових додатків, моніторинг, облік використання ресурсів. На рис. 1.7 представлена загальна типова архітектура хмари, запропонована в [10].

Рисунок 1.7 – Типова архітектура хмари, запропонована IBM

2 АУДИТ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Аудит інформаційної безпеки вважається одним з найбільш важливих напрямків стратегічного та оперативного менеджменту в області безпеки хмарних технологій. Він швидко розвивається. Його головне завдання - оцінити поточний стан інформаційної безпеки (ІБ) організації.

Під аудитом інформаційної безпеки розуміється системний процес отримання неупереджених високоякісних і кількісних оцінок поточного стану ІБ організації в узгодженні з певними аспектами й показниками на всіх основних рівнях забезпечення безпеки: нормативно-методологічному, організаційно-управлінському, процедурному і програмно-технічному.

Підсумки кваліфіковано виконаного аудиту ІБ організації дають можливість вибудувати кращу по продуктивності та витратам систему забезпечення інформаційної захищеності (СЗІБ), що являє собою комплекс технічних засобів, а ще процедурних, організаційних і правових заходів, об'єднаних на базі моделі управління ІБ.

В результаті проведення аудиту отримуються як якісні, так і кількісні оцінки. При оцінюванні, наприклад, є можливість скласти список вразливостей в програмно-апаратному забезпеченні з їх систематизацією за тришаровою шкалою загроз: найвища, середня і невисока. Кількісні оцінки найчастіше використовуються при оцінці ризику для активів організації. Оцінці можепідлягати вартість ризику, можливість ризику, величина ризику та ін.

Об'єктивність аудиту гарантується, зокрема, тим, що оцінка стану ІБ ведеться спеціалістами на базі конкретної системи, що дозволяє неупереджено вивчити всі елементи СЗІБ [2].

Розрізняють зовнішній і внутрішній аудит. Зовнішній аудит – це, як правило, разова подія, що проводиться з ініціативи управління організації або ж акціонерів. Рекомендовано проводити зовнішній аудит періодично. Для фінансових організацій і акціонерних товариств це вважається невідкладним завданням. Внутрішній аудит представляє собою постійну роботу, яка виконується на підставі «Положення про внутрішній аудит». Він затверджується управлінням організації. Цілями проведення аудиту захищеності інформаційної системи вважаються:

- тест ризиків, пов'язаних з імовірністю втілення небезпек захищеності щодо ресурсів ІС;
- оцінка поточного значення безпеки ІС;
- локалізація у просторі системи оборони ІС;
- оцінка співвідношення ІС наявним еталонам в області інформаційної безпеки;
- розробка призначень по впровадженню і збільшенню продуктивності пристроїв захищеності ІС [2].

2.1 Види аудиту інформаційної безпеки

Об'єктивність аудиту гарантується, зокрема, тим, що оцінка стану ІБ ведеться фахівцями на базі конкретної системи, що дозволяє об'єктивно вивчити всі елементи СЗІБ.

Аудит ІБ пропонують спеціальні компанії, втім в організації зобов'язаний проводитися свій внутрішній аудит ІБ. Він проводиться, наприклад, адміністраторами з безпеки.

Зазвичай виділяють три види аудиту ІБ, які відрізняються списком аналізованих компонент СЗІБ і одержуваними підсумками.

1) Поточний аудит.
2) Експертний аудит.
3) Аудит на відповідність еталонам ІБ.

Поточний аудит представляє собою обстеження стану безпеки конкретних підсистем інформаційної безпеки (ПІБ), що відносяться до програмно-технічних засобів. Наприклад, варіант інтенсивного аудиту, який іменується тестом на вторгнення. Він включає обстеження підсистеми оборони мережевих взаємодій. Поточний аудит складається з:

- теста поточної архітектури та опцій складових;
- інтерв'ювання кваліфікованих і зацікавлених осіб;
- проведення інструментальних перевірок, що охоплюють певні частини інфраструктури компанії;
- перевірки підсистем інформаційної безпеки.

Тест архітектури і опцій складових підсистеми інформаційної безпеки ведеться спеціалістами, які володіють знаннями про певні підсистеми, які входять

до складу системи. Підсумком цього аналізу вважається комплект опитувальних листів та інструментальних досліджень.

Опитувальні листи застосовуються в процесі інтерв'ювання осіб, відповідальних за адміністрування інформаційної системи. Наприклад, в опитувальні листи можуть бути включені питання, пов'язані з політикою заміни і призначення паролів, актуальним станом автоматичних інформаційних систем і ступенем критичності окремих її підсистем та бізнес-процесів організації в цілому.

Паралельно з інтерв'юванням ведуться інструментальні випробування які мають включати такі дії:

- зоровий огляд приміщень, обстеження системи контролю доступу в приміщення;
- отримання конфігурацій і версій приладів і ПЗ;
- дослідження співвідношення цих змін з наданими початковими даними;
- отримання карти мережі;
- застосування сканерів безпеки (універсальних, так і спеціалізованих);
- моделювання атак, що використовують уразливості системи;
- випробування реакції на атаки.

Аудитор має можливість використовувати різні моделі інформаційної системи.

1) Модель «чорного ящика» – аудитор не володіє практично ніякими апріорними знаннями про інформаційну систему, що досліджується. Наприклад, при проведенні зовнішнього інтенсивного аудиту, аудитор має можливість, беручи до уваги лише ім'я або IP адресу Web-сервера, спробувати відшукати уразливості в його захисті.

2) Модель «білого ящика» – аудитор має абсолютне знання про структуру мережі, що досліджується. Наприклад, аудитор має можливість володіти картою всієї або частини мережі, знання про операційну систему і існуючі додатки. Використання такої моделі не в абсолютній мірі імітує справжні впливи зловмисника, але дозволяє, втім, припустити «найгірший» сценарій, коли атакуючий має абсолютні дані про мережу.Такий підхід дає можливість побудувати сценарій інтенсивного аудиту таким чином, щоб інструментальні дослідження не приводили до затримок в її роботі.

3) Модель «кришталевого ящика» – аудитор імітує вплив внутрішнього користувача, який є власником облікового запису доступу в мережу з конкретним рівнем можливостей. Надана модель дозволяє розцінити небезпеки, пов'язані з внутрішніми небезпеками, наприклад від неблагонадійних службовців фірми.

За підсумками інтенсивного аудиту формується аналітична доповідь, що складається з опису поточного стану технічної частини СЗІБ, переліку відшуканих вразливостей в автоматичній інформаційній системі зі ступенем їх критичності і підсумків оцінки ризиків. Доповідь також включає модель порушника і модель небезпек. Додатково може бути розроблений проект з модернізації технічної частини СЗІБ, що складається зі списку призначень з обробки ризиків.

2.2 Етапність робіт з проведення аудиту безпеки інформаційної системи

Роботи з аудиту захищеності ІС містять ряд рубежів, які в цілому відповідають крокам проведення універсального аудиту, який включає в себе наступне:

- ініціювання процедури аудиту;
- збір детальної інформації аудиту;
- аналіз даних аудиту;
- вироблення призначень;
- підготовка аудиторського звіту.

Аудит ведеться не з ініціативи аудитора, а з ініціативи керівника фірми, який в даному питанні вважається провідною зацікавленою стороною. Допомога керівника фірми вважається важливою умовою для проведення аудиту.

Аудит представляє собою комплекс дій, в яких крім самого аудитора, залучені представники більшості структурних підрозділів фірми. Вплив всіх членів цього процесу повинен бути скоординований. На початку аудиту повинні бути вирішені належні організаційні питання.

1) Права і прямі обов'язки аудитора повинні бути точно визначені і документально закріплені в посадових інструкціях, а ще в Положенні про внутрішній аудит.

2) Аудитором повинен бути підготовлений і узгоджений з управлінням план проведення аудиту.

3) У положенні про внутрішній аудит повинно бути закріплено, зокрема, положення про те, що співробітники компанії зобов'язані надавати підтримку аудитору і надавати всю потрібну для проведення аудиту інформацію.

На кроці ініціювання процедури аудиту повинні бути визначені межі проведення обстеження. Одні інформаційні підсистеми фірми не вважаються досить критичними і їх можливо виключити з переліку проведення обстеження. Інші підсистеми можуть виявитися важкодоступними для аудиту через наявність грифу конфіденційності.

Межі проведення обстеження визначаються таким переліком:

- список фізичних, програмних та інформаційних ресурсів, що підлягають обстеженню;
- майданчики, що потрапляють в межі обстеження;
- основні види небезпек захищеності, що розглядаються при проведенні аудиту;
- організаційні (законодавчі, адміністративні та процедурні), програмно-технічні та інші нюанси забезпечення захищеності, які потрібно брати до уваги в ході проведення обстеження та їх цінність.

Проект і межі проведення аудиту дискутується на робочих зборах, в яких беруть участь аудитори та керівники структурних підрозділів.

Період збору інформації аудиту, як правило важкий і довгий. Це пов'язано часто з відсутністю важливої документації на інформаційну систему і з потребою взаємодії аудитора з майже всіма посадовими особами організації.

Компетентні висновки порівняльного стану справ у фірми з інформаційною захищеністю мають бути виготовлені аудитором лише тільки за умови присутності всіх важливих початкових даних для аналізу. Отримання інформації про організацію, функціонування та поточний стан ІС виконується аудитором в ході санкціонованих бесід з відповідальними особами фірми, методом дослідження технічної та організаційно-розпорядчої документації, а ще з вивчення ІС з впровадженням спеціального програмного засобу.

Забезпечення ІБ організації – це процес, що вимагає точної організації та дисципліни. Він зобов'язаний починатися з визначення ролей і розділення відповідальності між посадовими особами, що займаються ІБ організації. В наслідок цього на першому місці аудиторського обстеження є отримання

інформації про організаційну структуру користувачів ІС. У зв'язку з вищесказаним аудитору потрібна така документація.

1) Схема організаційної структури користувачів.

2) Схема організаційної структури обслуговуючого персоналу.

Як правило, в ході інтерв'ю аудитор задає опитуваним належні питання.

1) Питання про володарів інформації.

2) Питання про користувачів інформації.

3) Питання про інтернет-провайдерські послуги.

Призначення та основи функціонування ІС багато в чому визначають небезпеки та питання до захищеності системи. В наслідок цього на належному етапі аудитора цікавить інформація про призначення та функціонування ІС. Аудитор задає опитуваним приблизно належні питання.

1) Пропозиції і яким чином даються кінцевим користувачам.

2) Головні види додатків, що діють в ІС.

3) Кількість і коротка характеристика користувачів, які використовують ці програми.

Аудитору може буде потрібна ще така документація:

- функціональна схема;
- опис функцій автоматизації;
- опис провідних технічних рішень;
- інша проектна та робоча документація на інформаційну систему.

Далі, аудитору буде потрібно більш детальна інформація про структуру ІС. Це дозволить усвідомити, яким чином розподілені пристрої захищеності за структурними складовими та рівнями функціонування ІС. Типові питання, які обговорюються у зв'язку з цим під час інтерв'ю.

1) Питання про компоненти з яких складається ІС.

2) Питання про функціональність окремих компонентів.

3) Питання про знаходження меж системи.

4) Питання про точки входу в систему.

5) Питання про взаємодію ІС з іншими системами.

6) Питання про канали зв'язку які застосовуються для взаємодії з іншими ІС.

7) Питання про програмно-технічні платформи які застосовуються при побудові системи.

На наступному етапі аудитору потрібно мати данний перелік документів:

- структурну схему ІС;
- схему інформаційних потоків;
- опис структури комплексу технічних засобів інформаційної системи;
- опис структури програмного забезпечення;
- опис структури інформаційного забезпечення;
- розміщення компонент інформаційної системи.

Підготовка значущої частини документації на ІС, як правило, виконується вже в процесі проведення аудиту. Коли всі потрібні дані по ІС, включно з документацією, підготовлені, можливо перейти до їх аналізу.

Найважчий етап аналізу ґрунтується на аналізі ризиків. Роблячи упор на способи аналізу ризиків, аудитор визначає для обстежуваної ІС комплект заходів безпеки, який враховує особливості даної ІС та середовище її функціонування. На якість підсумків аудиту, в даному випадку, значно впливає методологія аналізу та управління ризиками і можливість її застосування до цього типу ІС.

Більш практичний етап, спирається на впровадження стереотипів ІБ. Стереотипи визначають базисний комплект заходів безпеки для широкого класу ІС, який складається в результаті узагальнення світової практики. Стереотипи мають різні набори заходів безпеки, в залежності від рівня безпеки ІС, який буде потрібно гарантувати. Від аудитора в даному випадку буде потрібно вірно кваліфікувати комплект заходів еталона, співвідношення з яким потрібно гарантувати для даної ІС. Важливий ще спосіб, що дозволяє оцінити це співвідношення. Описаний алгоритм більш поширений на практиці. Він дозволяє при найменших витратах ресурсів створювати аргументовані висновки про стан ІС.

Більш дієвий метод це комбінування перших двох. Базисний комплект заходів безпеки, що пред'являються до ІС, доповнюється заходами, що враховують особливості функціонування наданої ІС на базі аналізу ризиків. Даний розклад вважається набагато легше першого, тому що більша частка засобів захисту вже визначена стереотипом, і, разом з тим, він позбавлений недоліку другого розкладу, який не враховує специфіку реальної системи.

Аналіз ризиків – це те, з чого має починатися побудова будь-якої системи інформаційної безпеки. Він складається з заходів по обстеженняю безпеки ІС з метою визначення загроз, а також в якій мірі ті чи інші ресурси потребують

захисту. Визначення набору адекватних контрзаходів здійснюється в ході управління ризиками. Ризик визначається ймовірністю заподіяння шкоди і величиною збитку, що наноситься ресурсам ІС у разі здійснення загрози безпеці системи [11].

Аналіз ризиків полягає в тому, щоб їх виявити і оцінити їх значення (дати їм якісну, або кількісну оцінку). Процес аналізу ризиків можливо розділити слідуючі кроки.

1) Ідентифікація головних ресурсів ІС.

2) Визначення значущості тих або інших ресурсів для фірми.

3) Ідентифікація небезпек та вразливостей, що роблять ймовірним здійснення загроз.

4) Обчислення ризиків, пов'язаних з небезпеками.

Ресурси ІС можна поділити на наступні категорії:

- інформаційні ресурси;
- програмне забезпечення;
- технічні способи (сервери, робочіі станції, мережеве забезпечення і т.п.);
- людські ресурси.

Усі ресурси поділяються на класи та підкласи. Потрібно ідентифікувати лише тільки ті ресурси, які визначають працездатність ІС і важливі з точки зору забезпечення безпеки.

Важливість ресурсу оцінюється величиною шкоди, що наноситься в разі порушення конфідеційності або ж доступності до цього ресурсу. Як правило розглядаються наступні види шкоди:

- дані були відкриті, змінені, видалені або ж стали недоступні;
- апаратура була пошкоджена або ж зруйнована;
- порушено єдність програмного забезпечення.

Збиток може бути завдано організації в результаті успішного здійснення наступних видів загроз:

- локальні та віддалені атаки на ресурси ІС;
- стихійне лихо;
- помилки, або навмисні впливи персоналу ІС;
- збої в роботі ІС, викликані помилками в програмному забезпеченні або ж поломками апаратури.

Під вразливостями як правило розуміють якості ІС, що роблять ймовірним успішне втілення небезпек.

Розмір ризику обичлюється на базі ціни ресурсу, ймовірності втілення небезпеки та величини уразливості за формулою:

$$Р = \frac{Ц \cdot Й}{В} \tag{2.1}$$

де Р – ризик;

Ц – ціна ресурсу;

Й – ймовірність загрози;

В – величина вразливості.

Завдання управління ризиками полягає у виборі обґрунтованого комплекту контрзаходів, що дозволяють знизити значення ризиків до оптимальної величини. Ціна реалізації контрзаходів повинна бути меншою за величину ймовірної шкоди. Різниця між ціною реалізації контрзаходів і величиною ймовірної шкоди повинна бути обернено пропорційна ймовірності заподіяння шкоди.

У разі якщо для проведення аудиту безпеки обраний розклад, заснований на аналізі ризиків, то після аналізу даних аудиту, як правило, складаються належні групи завдань.

1) Аналіз ресурсів ІС, що охоплює інформаційні ресурси, програмні та технічні засоби і людські ресурси.

2) Аналіз груп завдань, що вирішуються системою і бізнес-процесів.

3) Побудова моделі ресурсів ІС, що визначає зв'язки між інформаційними, програмними, технічними та людськими ресурсами, їх обопільне місце розташування і методи взаємодії.

4) Оцінка критичності інформаційних ресурсів, а також програмних і технічних засобів.

5) Визначення критичності ресурсів з урахуванням їх взаємозалежностей.

6) Визначення можливих небезпек щодо ресурсів ІС і вразливостей оборони, що роблять ймовірним втілення атак.

7) Оцінка ймовірності втілення атак, величини вразливостей і шкоди, що наноситься організації в разі вдалого втілення небезпек.

8) Визначення величини ризиків для будь-якого елементу трійки: небезпека-група ресурсів-вразливість.

9) Перерахований комплект завдань, вважається загальним. Для їх укладення мають всі шанси застосовуватися всілякі формальні та неформальні, кількісні та якісні, ручні та автоматичні способи аналізу ризиків. Сутність підходу від цього не змінюється.

Оцінка ризиків може бути розрахована по кількісним шкалам. На базі такого аналізу повинна бути розроблена система першочергових дій щодо зменшення величини ризиків до допустимого значення.

У разі проведення аудиту безпеки на співвідношення до вимог еталону, аудитор, покладаючись на особистий навик, розглядає можливість застосування вимог еталона до обстежуваної ІС. Дані про відповідність різних областей функціонування ІС вимогам еталону, як правило, представляються в табличній формі. З таблиці видно, які запити безпеки в системі не забезпечені. Виходячи з цього, робляться висновки про відповідність обстежуваної ІС вимогам еталону і надаються поради щодо реалізації в системі пристроїв безпеки, які дозволяють гарантувати це співвідношення.

Рекомендації аудитора зобов'язані бути застосованими до ІС. Вони також повинні бути економічно обґрунтованими, аргументованими (підкріпленими підсумками аналізу) і відсортованими за ступенем значущості.

Аудиторський звіт є основним результатом проведення аудиту. Його якість характеризує якість роботи аудитора. Структура звіту може істотно відрізнятися в залежності від характеру і цілей проведеного аудиту. Однак певні розділи повинні обов'язково бути присутніми в аудиторському звіті. Він повинен, обов’язково, містити опис цілей проведення аудиту, характеристику обстежуваної ІС, вказівку меж проведення аудиту і методів, що використовувалися, результати аналізу даних аудиту, висновки, що узагальнюють ці результати і містять оцінку рівня захищеності АС або відповідність її вимогам стандартів, і, звичайно, рекомендації аудитора щодо усунення існуючих недоліків і вдосконалення системи захисту.

Для прикладу, наведемо зразок структури аудиторського звіту за результатами аналізу ризиків, пов'язаних із здійсненням загроз безпеці щодо обстежуваної ІС. Структура звіту за результатами аудиту безпеки ІС та аналізу ризиків.

Вступна частина:

- введення (цілі та завдання проведення аудиту);
- опис ІС;
- призначення та основні функції системи (групи завдань, що вирішуються в системі);
- класифікація користувачів ІС;
- організаційна структура обслуговуючого персоналу ІС;
- структура і склад комплексу програмно-технічних засобів ІС (види інформаційних ресурсів, що зберігаються і обробляються в системі);
- структура інформаційних потоків;
- характеристика каналів взаємодії з іншими системами і точок входу;
- методика проведення аудиту;
- методика аналізу ризиків;
- вихідні дані.

Оцінка критичності ресурсів ІС:

- критерії оцінки величини можливого збитку, пов'язаного із здійсненням загроз безпеки;
- оцінка критичності інформаційних ресурсів;
- класифікація інформаційних ресурсів;
- оцінка критичності за групами інформаційних ресурсів;
- оцінка критичності технічних засобів;
- оцінка критичності програмних засобів;
- модель ресурсів, що описує розподіл ресурсів по групах завдань.

Аналіз ризиків, пов'язаних із здійсненням загроз безпеці щодо ресурсів ІВ:

- модель порушника інформаційної безпеки;
- модель внутрішнього порушника;
- модель зовнішнього порушника;
- модель загроз безпеці та вразливостей інформаційних ресурсів;
- загрози безпеки, спрямовані проти інформаційних ресурсів;
- загрози несанкціонованого доступу до інформації за допомогою програмних засобів;
- загрози, що здійснюються з використанням штатних технічних засобів;
- загрози, пов'язані з витоком інформації по технічним каналам;
- загрози безпеки, спрямовані проти програмних засобів;

- загрози безпеки спрямовані проти технічних засобів;
- оцінка серйозності загроз безпеці і величини вразливостей;
- критерії оцінки серйозності загроз безпеці і величини вразливостей;
- оцінка серйозності загроз;
- оцінка величини вразливостей;
- оцінка ризиків для кожного класу загроз і групи ресурсів.

За результатами обстеження формулюються рекомендації:

- рекомендовані контрзаходи організаційного рівня;
- рекомендовані контрзаходи програмно-технічного рівня.

2.3 Програмні продукти для аналізу та управління ризиками

В наш час існує велика кількість програмних засобів аналізу та управління ризиками. Розглянемо приклади деяких, більш популярних. Першим розглянемо CRAMM.

Програма CRAMM була розроблена Службою безпеки Великобританії за завданням британського уряду і взята на озброєння в якості муніципального еталона. Вона застосовується, починаючи з 1985 р. урядовими та платними організаціями Великобританії. За цей час CRAMM стала популярною у всьому світі. Компанія Insight Consulting Limited займається розробкою і супроводом схожого програмного продукту, що реалізує спосіб CRAMM.

В наш час CRAMM – це досить потужний і універсальний інструмент, що дозволяє, крім аналізу ризиків, вирішувати ще й ряд інших аудиторських завдань.

1) Проведення обстеження ІС та випуск супровідної документації на всіх кроках його проведення.

2) Проведення аудиту в узгодженні з еталоном BS 7799: Code of Practice for Information Security Management BS7799.

3) Розробка забезпечення безперервності бізнесу.

В основі програми CRAMM лежить набір засобів для оцінки ризиків, що комбінує кількісні та якісні способи аналізу. Спосіб є універсальним і підходить як для великих, так і для малих організацій, як урядового, так і приватного типу. Версії програмного забезпечення CRAMM, спрямовані на різні типи організацій, різняться власними базами знань (profiles). Для приватних організацій наявний платний профіль (Commercial Profile), для урядових організацій – урядовий

профіль (Government profile). Урядовий варіант профілю дозволяє проводити аудит на відповідність вимогам південноамериканського еталона ITSEC («Помаранчева книга») [12].

Грамотне впровадження способу CRAMM дозволяє отримувати досить непогані результати, найбільш важливимим з яких, напевно, є ймовірність фінансового обґрунтування витрат організації на забезпечення інформаційної безпеки та безперервності бізнесу. Економічно обґрунтована стратегія управління ризиками дозволяє, в кінцевому результаті уникати невиправданих витрат.

У програмі CRAMM вся процедура ділиться на три кроки. Завданням першого кроку вважається відповідь на питання: «чи достатньо для захисту системи використання засобів базисного значення, що реалізують класичні функції безпеки, або ж потрібно проведення більше деталізованого аналізу?» На другому кроці виконується ідентифікація ризиків і оцінюється їх розмір. На 3-му кроці приймається рішення про вибір адекватних контрзаходів.

Спосіб CRAMM для будь-якого кроку визначає комплект початкових даних, черговість дій, анкети для проведення інтерв'ю, переліки випробування і комплект звітних документів.

У разі, якщо за підсумками проведення першого кроку, встановлено, що ступінь критичності ресурсів досить невисока і небезпека не перевищить базисного значення, то до системи застосовується найменший комплект засобів безпеки. В даному випадку більша частка дій другого кроку не проводиться, а виконується перехід до третього кроку, на якому генерується звичайний перелік контрзаходів для забезпечення базисного набору засобів безпеки.

На другому кроці виконується тест небезпек та вразливостей. Початкові дані для оцінки небезпек і вразливостей аудитор отримує від уповноважених співробітників організації в ході належних інтерв'ю. Для проведення інтерв'ю застосовуються спеціальні опитувальники.

На 3-му кроці приймається рішення про управління ризиками, що полягає у виборі адекватних контрзаходів.

Висновок про впровадження в систему нових пристроїв безпеки та трансформація існуючих вписується в інструкцію організації. При цьому береться до уваги рівень витрат, їх прийнятність і кінцеву вигоду для бізнесу. Завданням аудитора вважається обґрунтування відповідних контрзаходів для управління організації.

У разі прийняття висновку про впровадження нових контрзаходів і трансформації існуючих, на аудитора покладається завдання підготовки нових контрзаходів та оцінки продуктивності їх застосування. Висновок якості результтів виходить за рамки способу CRAMM.

Концептуальна схема проведення обстеження за способом CRAMM показана на рис. 2.1.

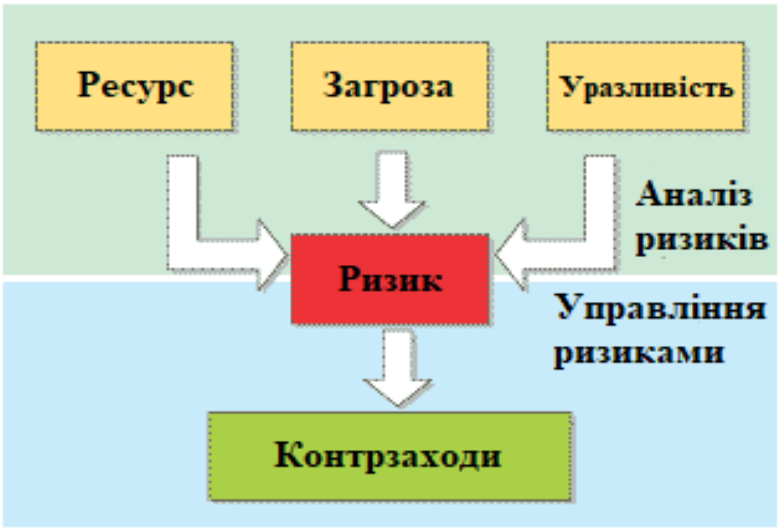

Рисунок. 2.1 – Концептуальна схема проведення обстеження за способом CRAMM

Процедура аудиту в способі CRAMM вважається формалізованою. На будь-якому етапі генерується досить величезна кількість проміжних і результуючих результатів.

На першому етапі формуються:

- модель ресурсів, що має опис ресурсів, які потрапляють в межі вивчення, і взаємозв'язків між ними;
- оцінка критичності ресурсів;
- результуюча доповідь по першому кроку аналізу ризиків, в якому підсумовуються підсумки, отримані в ході обстеження.

На другому етапі проведення обстеження формуються слідуючі види доповідей:

- результати оцінки значення небезпек і вразливостей;
- результати оцінки величини ризиків;
- результуюча доповідь по другому кроку аналізу ризиків.

За підсумками третього кроку обстеження формуються такі види доповідей:

- рекомендовані контрзаходи;
- детальна специфікація безпеки;
- оцінка ціни відповідних контрзаходів;
- список контрзаходів, відсортованих в узгодженні з їх пріоритетами;
- результуюча доповідь по третьому кроку обстеження;
- політика безпеки, що містить опис заходів безпеки, стратегій і основ захисту ІС;
- список дій по забезпеченню безпеки.

Компетентно використовувати спосіб CRAMM в змозі лише тільки висококваліфікований аудитор, який пройшов навчання. У разі, якщо організація не має можливості для себе дозволити тримати в штаті спеціаліста по захисту, то найбільш вірним висновком стане запрошення аудиторської компанії, що володіє штатом знавців, які мають практичний навик використання способу CRAMM.

До позитивних сторін способу CRAMM відносяться:

- CRAMM вважається якісним способом аналізу ризиків, що дозволяє отримувати достовірні практичні результати;
- програмний інструментарій CRAMM можна застосовуватися на всіх стадіях проведення аудиту безпеки ІС;
- у основіі програмного продукту лежить досить велика база знань з контрзаходів в області інформаційної безпеки, заснована на настановах еталона BS 7799;
- гнучкість і універсальність способу CRAMM дозволяє застосувати його для аудиту ІС різних типів;
- CRAMM можливо застосувати в якості інструменту для забезпечення розробки безперервності бізнесу;
- CRAMM дає можливість документування пристроїв безпеки ІС.

До недоліків способу CRAMM треба віднести:

- використання способу CRAMM вимагає особливої підготовки та найвищої кваліфікації аудитора;
- CRAMM в значно більшій мірі підходить для аудиту ІС, які знаходяться на стадії експлуатації ніж для ІС, що опинилися на стадії розробки;
- аудит за способом CRAMM досить трудовитратний і потребує місяців роботи аудитора;

- програмний інструментарій CRAMM генерує величезну кількість бумажної документації, яка не завжди потрібна на практиці;
- CRAMM не дозволяє робити особисті шаблони доповідей або ж видозмінювати наявні;
- можливість внесення доповнень в основу знань CRAMM не доступна звичайним користувачам.

Програмне забезпечення RiskWatch, що розроблено американською компанією RiskWatch. Inc., є потужним засобом аналізу та управління ризиками. У сімейство RiskWatch входять програмні продукти для проведення різних видів аудиту безпеки. Воно містить наступні засоби аудиту та аналізу ризиків:

- RiskWatch for Physical Security – для фізичних методів захисту ІС;
- RiskWatch for Information Systems – для інформаційних ризиків;
- HIPAA-WATCH for Healthcare Industry – для оцінки відповідності вимогам стандарту HIPAA;
- RiskWatch RW17799 for ISO 17799 – для оцінки вимогам стандарту ISO 17799.

У методі RiskWatch в якості критеріїв для оцінки та управління ризиками використовуються передбачення річних втрат ALE і оцінка «повернення від інвестицій» ROI. Сімейство програмних продуктів RiskWatch, має масу переваг. До недоліків даного продукту можна віднести його відносно високу вартість [13].

Використовується також система Cobra (консультативний об'єктивний та функціональний аналіз ризиків), що розроблена компанією risk Associates, ISO 17799. Cobra реалізує методи кількісної оцінки ризиків, а також інструменти для консалтингу та проведення оглядів безпеки. При розробці інструментарію Cobra були використані принципи побудови експертних систем, велика база знань з загроз і вразливостей, а також велика кількість переліків запитань, з успіхом застосовуються на практиці. Для роботи з сімейством програмних продуктів Cobra Consultant Cobra ISO 17799 потрібні: консультант з безпеки, аналітик відповідності політики Cobra і консультант із захисту даних Cobra.

Програмний продукт Buddy System, що розроблений компанією Countermeasures Corporation, є ще одним програмним продуктом, що дозволяє здійснювати як кількісний, так і якісний аналіз ризиків. Він містить розвинені засоби генерації звітів. Основний акцент при використанні Buddy System робиться

на інформаційні ризики, пов'язані з порушенням фізичної безпеки та управління проектами.

2.4 Стандарти, що використовуються при проведенні аудиту безпеки інформаційних систем

У цьому розділі розглядаються стандарти інформаційної безпеки, які є найбільш значущими та перспективними з точки зору їх використання для проведення аудиту безпеки ІС. Наслідком проведення аудиту, все частіше стає сертифікат, що засвідчує відповідність обстежуваної ІС вимогам визнаного міжнародного стандарту. Наявність такого сертифіката дозволяє організації отримувати конкурентні переваги, пов'язані з великою довірою з боку клієнтів і партнерів. Значення міжнародних стандартів ISO17799 та ISO15408 важко переоцінити. Ці стандарти служать основою для проведення будь-яких робіт в області інформаційної безпеки, в тому числі та аудиту. ISO17799 зосереджений на питаннях організації та управління безпекою, в той час як ISO15408 визначає детальні вимоги, що пред'являються до програмно-технічних механізмів захисту інформації.

Специфікація SysTrust в даний час досить широко використовується аудиторськими компаніями, які традиційно виконують фінансовий аудит для своїх клієнтів і пропонують послугу IT аудиту в якості доповнення до фінансового аудиту. Німецький стандарт "BSI\IT Baseline Protection Manual" містить змістовне керівництво по забезпеченню безпеки IT, що і представляє практичну цінність для всіх фахівців, які займаються питаннями інформаційної безпеки. Практичні стандарти та керівництва по забезпеченню інформаційної безпеки, що розробляються в рамках проекту SCORE, орієнтовані на технічних фахівців і є в технічному плані найбільш досконалими в даний час.

Програма сертифікації інтернет-сайтів за вимогами інформаційної безпеки та відповідна специфікація "SANS\GIAC Site Certification", запропонована інститутом SANS. Вона заслуговує розгляду у зв'язку з незмінно зростаючою актуальністю питань захисту ІС організацій від атак з боку мережі Інтернет.

Для оцінки пристроїв захищеності організаційного значення розроблений еталон ISO 17799: Code of Practice for Information Security Management, прийнятий у 2000 році. ISO 17799 був розроблений на базі англійського еталона BS 7799. ISO

17799 і може застосовуватися в якості критеріїв для оцінки захищеності пристроїв організаційного значення, охоплюючи адміністративні, процедурні та фізіологічні заходи захисту. Практичні критерії розбиті на 10 розділів.

1) Політика захищеності.
2) Організація захисту.
3) Класифікація ресурсів та їх контроль.
4) Безпека персоналу.
5) Фізична захищеність.
6) Адміністрування комп'ютерних систем і обчислювальних мереж.
7) Управління доступом.
8) Розробка та супровод інформаційних систем.
9) Планування безперебійної роботи організації.
10) Контроль виконання заходів захищеності.

Десять засобів контролю, за пропонованих в ISO 17799 позначені як ключові, вважаються найбільш актуальними. Під способами контролю в наданому контексті розуміються механізми управління інформаційною захищеністю організації.

Ключовими для захисту інформації можна вважати такі методи:

- підготовка персоналу до підтримання режиму інформаційної безпеки;
- повідомлення про випадки порушення захисту;
- способи захисту від комп’ютерних вірусів;
- планування безперебійної роботи організації;
- контроль над копіюванням програмного забезпечення, захищеного законодавством про авторське право;
- захист документації організації.

Аспекти для оцінки пристроїв захищеності програмно-технічного значення представлені в інтернаціональному еталоні ISO 15408 Common Criteria for Information Technology Security Evaluation.

Німецький стандарт - це керівництво по забезпеченню безпеки IT базового рівня "IT Baseline Protection Manual" розроблене Агентством інформаційної безпеки Німеччини BSI – Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency).

Цей документ є, мабуть, найбільш змістовним керівництвом з інформаційної безпеки й за багатьма параметрами перевершує всі інші стандарти.

Цей найцінніше для аудитора джерело інформації, що є у вільному доступі в мережі Інтернет. У ньому міститися докладні керівництва по забезпеченню інформаційної безпеки стосовно до різних аспектів функціонування ІС в різних областях ІТ.

Цей стандарт в даний час займає три томи та містить близько 1600 сторінок тексту.

"BSI IT Baseline Protection Manual" постійно вдосконалюється з метою забезпечення його відповідності поточному стану справ в області безпеки ІТ. До теперішнього часу накопичена унікальна база знань, що містить інформацію з загроз і контрзаходів в добре структурованому вигляді.

SCORE є спільним проектом Інституту SANS і Центру безпеки інтернет CIS. Професіонали-практики в галузі інформаційної безпеки з різних організацій об'єдналися в рамках проекту SCORE з метою розробки базового (мінімально необхідного) набору практичних стандартів і посібників із забезпечення безпеки для різних операційних платформ. Вимоги та рекомендації, запропоновані для включення в стандарти, широко обговорюються і перевіряються учасниками проекту SCORE, і тільки після їх схвалення всіма учасниками, передаються в CIS, який займається їх формалізацією та оформленням, а також розробляє програмні засоби для оцінки відповідності операційних платформ запропонованим стандартам.

Розроблені базові стандарти разом з посібниками щодо забезпечення відповідності цим стандартам і засобами тестування публікуються на інтернет-сайті CIS.

Програма сертифікації інтернет-сайтів GIAC Site Certification program, що запропонована інститутом SANS, дозволяє організаціям проводити аудит безпеки сегментів комп'ютерної мережі, безпосередньо підключених до мережі Інтернет, відповідно до стандартів SCORE.

Програма сертифікації GIAC Site Certification визначає три рівні захищеності інтернет-сайтів. На практиці, в даний час, використовуються тільки перші два з них [14].

Сертифікація сайту на першому рівні передбачає перевірку зовнішніх мережевих адрес організації, видимих з мережі Інтернет на предмет уразливості відповідних хостів щодо мережевих атак. На цьому рівні повинен бути забезпечений захист сайту від найбільш поширених атак. При використанні цього

продукту пред'являються певні вимоги до рівня кваліфікації фахівців, що відповідають за забезпечення безпеки сайту.

На другому рівні потрібне проведення всіх перевірок і дотримання всіх вимог першого рівня, а крім того потрібно здійснювати періодичний перегляд політики та процедур забезпечення мережевої безпеки. Також на другому рівні проводиться перевірка захищеності сайту від мережевих атак шляхом здійснення спроб проникнення і взлому систем, підключених до мережі Інтернет.

На третьому рівні, крім забезпечення відповідності всім вимогам другого рівня, потрібно також регулярно проводити сканування мережі зсередини з метою захисту від загроз з боку внутрішніх порушників, а також зовнішніх зловмисників, які намагаються подолати механізми захисту зовнішнього периметра мережі шляхом використання просунутих методів, включаючи методи соціального інжинірингу.

3 АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ З ХМАРНОЮ ТЕХНОЛОГІЄЮ З ВИКОРИСТАННЯМ МЕТОДУ ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ

В цьому розділі доведено можливість використання штучної нейронної мережі для проведення експертного аудиту на основі чисельного оцінювання оперативного значення ризику порушення інформаційної безпеки (ІБ) мережі з хмарною технологією. Наведені умови вибору розміру даних навчальної вибірки для хорошої натренованості інформаційної штучної нейронної мережі (ШНМ). Розглянута архітектура нейронної мережі і оцінені можливі алгоритми навчання ШНС для вирішення поставленого завдання.

3.1 Проведення аудиту з точки зору системного аналізу

Аудит інформаційної безпеки – один з аспектів управління ІБ. Аудит доцільно проводити після розробки системи забезпечення інформаційної безпеки (СЗІБ) для оцінювання результатів проектування. Аудит проводиться періодично в ході експлуатації інформаційної системи (ІС) для оцінки ефективності існуючих заходів захисту, Активний аудит проводиться при розслідуванні інцидентів ІБ в режимі реального часу.

Якість аудиту безпеки залежить від адекватності інформації про об'єкт оцінки: відомостей про топологію мережі, відомостей про інфраструктуру інформаційної системи, про встановлені засоби захисту, про політику інформаційної безпеки, про програмне забезпечення та схему інформаційних потоків.

Аудит порушення ІБ забезпечує отримання та оцінку об'єктивних даних про поточний стан захищеності інформаційної системи. Необхідність здійснення аудиту безпеки пов'язана зі складністю інфраструктури сучасних ІС, безліччю додатків, що використовуються; об’ємом даних, що обробляється; складністю реалізації системи інформаційної безпеки та необхідністю обліку потенційно можливих загроз.

В атестаційній роботі під аудитом безпеки ІС з хмарною технологією розуміється експертиза стану захищеності, що включає отримання об'єктивних

даних про параметри та умови функціонування системи, які можуть впливати на захищеність. А також аналіз цих даних. В результаті експерт виявляє наскільки раціонально вирішені питання безпеки інформації та контролю доступу і як мінімізувати ризики при обробці в ІС конфіденційної інформації замовника, виявляє локалізацію слабких місць в системі забезпечення інформаційної безпеки та видає рекомендації про шляхи розв'язання існуючих проблем.

Для здійснення процедури аналізу вихідних даних аудитор може застосувати методику, яка дозволила б оцінити відповідність механізмів забезпечення інформаційної безпеки вимогам існуючих стандартів.

Інший підхід до проведення аналізу в ході аудиту заснований на оцінці ризиків. У цьому випадку повинні бути ідентифіковані всі можливі загрози, виявлені та оцінені уразливості. Експерт в аудиторському звіті вказує метод розрахунку інформаційних ризиків, що використаний при аудиті.

Враховуючи, що загрози порушення ІБ характеризуються багатоаспектністю подій, що відбуваються та альтернативністю сценаріїв, то проблему проведення експертного аудиту ІБ можна віднести до числа складних слабоструктурованих і слабо формалізуємих проблем.

У науці є досвід щодо розв'язання подібних проблем, що слабо формалізуються - це системний аналіз об'єктів дослідження [15]. Його позитивна риса обумовлена тим, що він є методом який дозволяє врахувати при розв'язання проблеми всі найбільш важливі фактори [16].

Методи системного аналізу це: декомпозиція, аналіз і синтез системи. У процесі дослідження рівня безпеки системи використовуються основні принципи системного аналізу стосовно до процесу проведення аудиту ІБ відносяться:

- розробка політики безпеки системи;
- розробка моделі загроз порушення ІБ;
- розробка архітектури та навчання ШНМ і отримання чисельних значень оперативного рівня ризику порушення інформаційної безпеки.

Для вирішення останнього завдання необхідно виконати наступні етапи.

1) Сформувати множину даних навчальної вибірки для налаштування параметрів штучної нейронної мережі.

2) Здійснити вибір ефективного алгоритму навчання штучної нейронної мережі.

3) Розробити програмний модуль для отримання чисельних значень оперативного рівня ризику порушення ІБ за допомогою нейронної мережі.

3.2 Розробка методу та структурної схеми, що реалізує метод проведення експертного аудиту інформаційної безпеки в системі хмарних обчислень

Система хмарних обчислень є інформаційною системою взаємодії споживача і постачальника хмарних послуг. З точки зору інформаційної безпеки в процесі забезпечення виконання бізнес-процесів такої системи можуть виникнути загрози ІБ, пов'язані з втратою довіри споживача до постачальника. Ці загрози виникають через відсутність вірогідного оцінювання рівня довіри до постачальника хмарних послуг у зв'язку із закритістю для користувачів застосовуваних постачальником хмарних технологій і програмних рішень. Крім того, користувачі хмарних послуг не володіють можливістю дати оцінку реалізованого рівня захищеності інформації, досягнутої постачальником.

В даному випадку необхідне проведення незалежного аудиту СЗІБ з подальшим наданням результатів споживачеві в якості гаранта збереження його критичної інформації.

Однією з переваг використання хмарних послуг є можливість здійснення вибору і зміни початкового складу програмного забезпечення (ПЗ) вже після введення системи хмарних обчислень в експлуатацію. Однак в цих умовах система, що розглядається як захищена на етапі проектування, після введення її в експлуатацію може мати безліч вразливостей, що містяться в новому ПЗ. Таким чином, можна зробити висновок про необхідність проведення періодичного незалежного аудиту інформаційної безпеки СЗІБ.

Проведення аудиту ІБ на сьогодні стає все більш затребуваною на ринку послуг інформаційної безпеки не тільки в хмарних середовищах, але і в традиційних інформаційних мережах.

Аудит ІБ є сукупністю трьох найважливіших складових.

1) Методології аудиту, що містить моделі, засоби та методи проведення аудиту.

2) Результат проведення аудиту (якісний або кількісний).

3) Еталонна система забезпечення ІБ, з якою порівнюються результати перевірки інформаційної системи.

Взаємозв'язок цих трьох компонентів аудиту ІБ представлений на рис. 3.1.

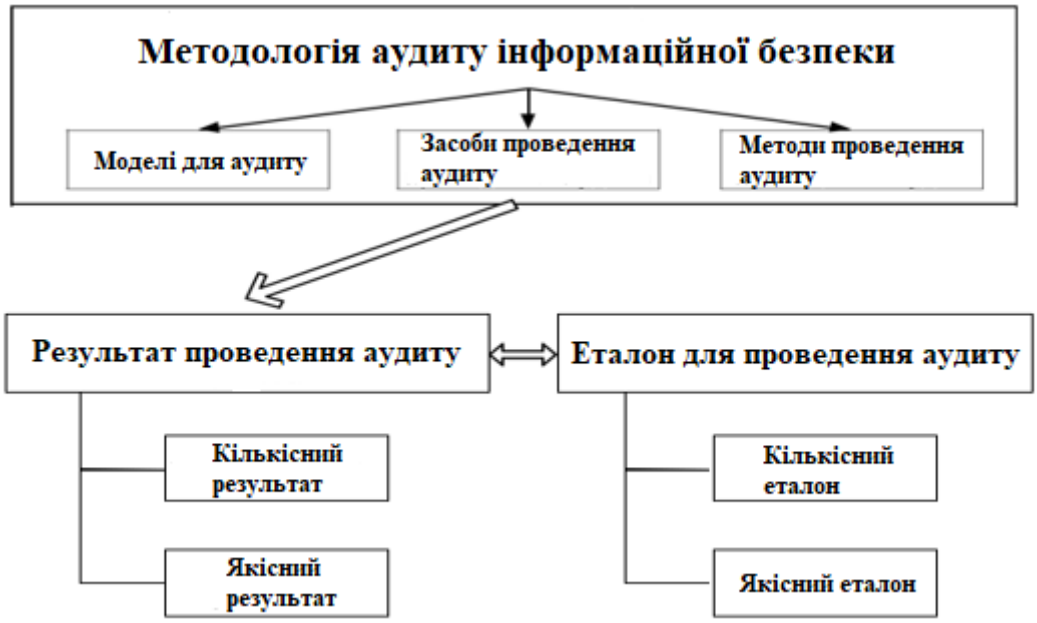

Рисунок 3.1 – Складові аудиту інформаційної безпеки

Якість проведеного аудиту безпеки багато в чому залежить від повноти та точності інформації, яка була отримана в процесі збору вихідних даних. Тому інформація повинна містити: існуючу організаційно-розпорядчу документацію, що стосується питань інформаційної безпеки; відомості про програмно-апаратне забезпечення системи, а також інформацію про засоби захисту, встановлені в ІС.

Розрізняють два види аудиту ІБ систем. Інструментальний (активний) аудит – виявлення вразливостей програмного та апаратного забезпечення систем засобами автоматизованої перевірки. Результатом активного аудиту є інформація про вразливості системи захисту інформації, ступеня їх критичності, а також, у ряді випадків, методи її усунення. Після закінчення активного аудиту видаються рекомендації щодо модернізації системи захисту інформації, які дозволяють усунути уразливості системи захисту інформації та тим самим підвищити рівень захищеності інформаційної системи в цілому. Як недолік активного аудиту є те, що без проведення інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення максимально ефективної системи захисту інформації.

Експертний аудит інформаційної безпеки підрозділяється на аудит відповідності вітчизняним стандартам інформаційної безпеки, при якому стан інформаційної безпеки порівнюється з якимось абстрактним описом, що

наводиться в стандартах, і на експертний аудит, метою якого є дослідити рівень захищеності системи.

Основним недоліком і відкритим питанням при проведенні аудиту ІБ на відповідність стандартам є питання про стандарти безпеки, перевірку на відповідність яким буде виконувати аудитор. Крім того, якщо стандарти в області ІБ відсутні або знаходяться на стадії розробки, то провести аудит на відповідність стандартам стає неможливим. У такому випадку єдиним способом проведення експертного аудиту є дослідження рівня захищеності системи, при цьому аудитор повинен використовувати методологію, що дозволяє провести оцінку ризиків порушення інформаційної безпеки системи.

У міжнародних стандартах в області інформаційної безпеки сформовані вимоги до методології оцінювання ризиків порушення ІБ [17]. Методологія повинна забезпечувати отримання чисельних значень рівня ризику, допомагати здійснювати внутрішній аудит для обґрунтування вибору коригувальних дій в процесі менеджменту захисту інформації, забезпечувати здатність до швидкої адаптації при зміні компонентів інфраструктури, повинна гарантувати, що метод оцінки ризиків дає порівнянні та зіставні результати.

На сьогодні відсутня методологія експертного аудиту ІБ, яка задовольняла б усім перерахованим вище вимогам. Що стосується рекомендацій і методик експертного аудиту ІБ в системі хмарних обчислень, то вони відсутні в законодавчих актах країн світу.

Методологія аудиту інформаційної безпеки системи повинна враховувати множинність суб'єктів і об'єктів атаки, флуктуації в часі системи хмарних обчислень. Методологія повинна забезпечувати найбільш ймовірні чисельні результати проведення аудиту навіть при можливій відсутності деяких необхідних для розрахунків вхідних даних. На сьогодні найбільш ефективним інструментом для рішення подібних завдань є сучасні інтелектуальні системи, серед яких можна виділити штучні нейронні мережі.

Штучна нейронна мережа – це самонавчальна інтелектуальна інформаційна система, яка будує асоціативну мережу понять (нейронів) для паралельного пошуку рішень за допомогою навчання на безлічі даних навчальної вибірки

В результаті навчання будуються математичні вирішальні функції (передавальні функції або функції активації), які визначають залежності між вхідними та вихідними сигналами нейронної мережі.

Штучний нейрон – це елементарний перетворювальний елемент, що має непорожню безліч входів, на які надходять сигнали (вхідні дані). На першому етапі в нейрон від інших нейронів приходить якесь число сигналів, обробивши їх, нейрон передає вихідний сигнал далі, іншому нейрону. На другому етапі сумарне збудження пропускається через активаційну функцію в результаті чого виходить вихідний сигнал нейрона. Узагальнена структура нейрона представлена на рис. 3.2.

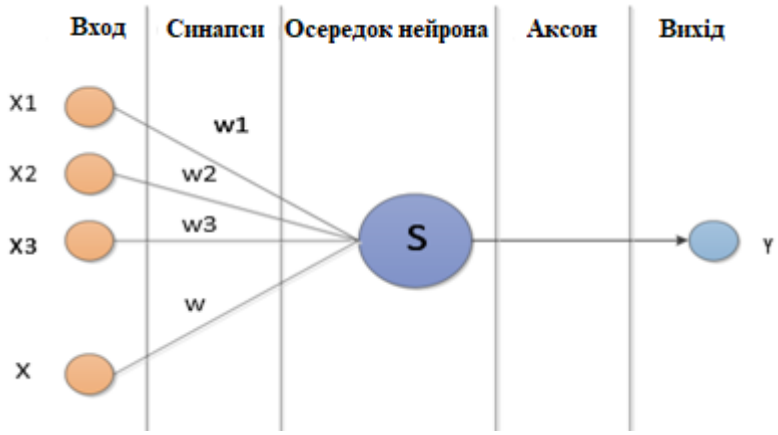

Рисунок 3.2 – Структура нейрона

На рисунку позначено: синапс – односпрямований вхідний зв'язок нейрона, поєднаний з виходом іншого нейрона, який має свою вагу; аксон – єдиний відросток біологічного нейрона, по якому він передає свій вихідний сигнал.

Навчання нейронної мережі зводиться до визначення зв'язків (синапсів) між нейронами та встановлення сили цих зв'язків (вагових коефіцієнтів). Алгоритми навчання нейронної мережі спрощено зводяться до визначення залежності вагового коефіцієнта зв'язку двох нейронів від числа прикладів, що підтверджують цю залежність.

Процес вирішення завдань навчання в силу проведення матричних перетворень проводиться дуже швидко і досить точно, що є безсумнівною перевагою нейронних мереж в порівнянні з іншими системами. У штучній нейронній мережі фактично імітується паралельний процес проходу нейронною мережею на відміну від послідовного в інших системах. Крім того, нейронні мережі легко можуть бути реалізовані у вигляді програмного модуля з асоціативною пам'яттю, що дозволяє автоматизувати розв'язувані завдання.

Розроблена методологія використовує теорію штучних нейронних мереж, а також безліч даних навчальної вибірки, створених на основі розрахункових даних за методом оцінки ризиків, запропонованого в [18].

Оцінка прогнозованого значення ризику пов'язана зі стратегією безпеки, яка розробляється для СЗІБ завчасно. В ході моніторингу безпеки системи забезпечується отримання інформації про стан мережевих пристроїв в хмарі, про події, що порушують безпеку, в реальному масштабі часу. При виявленні атаки або виявленні таких подій в СЗІБ необхідні тактичні дії. Тактичні дії повинні бути результатом організованої взаємодії систем моніторингу та управління пристроями мережевої безпеки. Прийняти рішення про те, які саме тактичні дії необхідно застосовувати в даний конкретний момент часу, допоможе чисельне оперативне значення рівня ризику. Взаємозв'язок понять прогнозованого та оперативного ризику показаний на рис. 3.3.

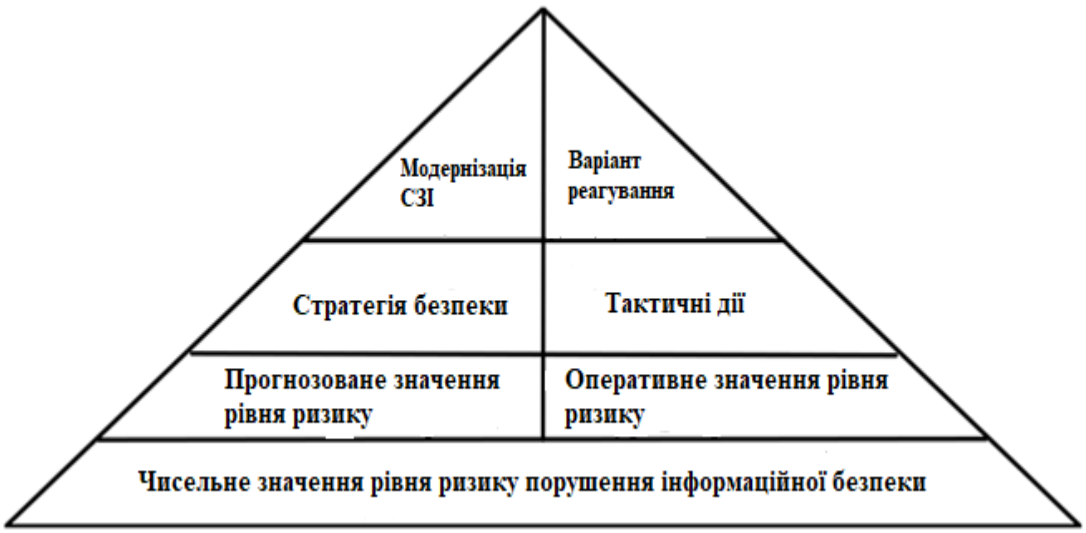

Рисунок 3.3 – Взаємозв'язок прогнозованого та оперативного значення рівня ризику порушення інформаційної безпеки

Результати розрахункових прогнозованих значень ризику використовуються в якості множини даних навчальної вибірки для ШНМ. На виходах нейронної мережі аудитор отримає оперативне значення ризику в реальному масштабі часу.

Таким чином, метод експертного аудиту на основі ШНМ містить наступні етапи:

- побудова моделі загроз;
- розрахунок прогнозованих значень рівня ризику порушення інформаційної безпеки системи хмарних обчислень;

- формування множини даних навчальної вибірки для навчання штучної нейронної мережі, налаштування та навчання ШНМ;
- визначення оперативного значення рівня ризику аудитором в реальному масштабі часу на основі даних з датчиків подій;
- формування звіту аудитора на основі отриманих значень рівня ризику.

Метод експертного аудиту ІБ системи хмарних обчислень, показаний на схемі рис. 3.4.

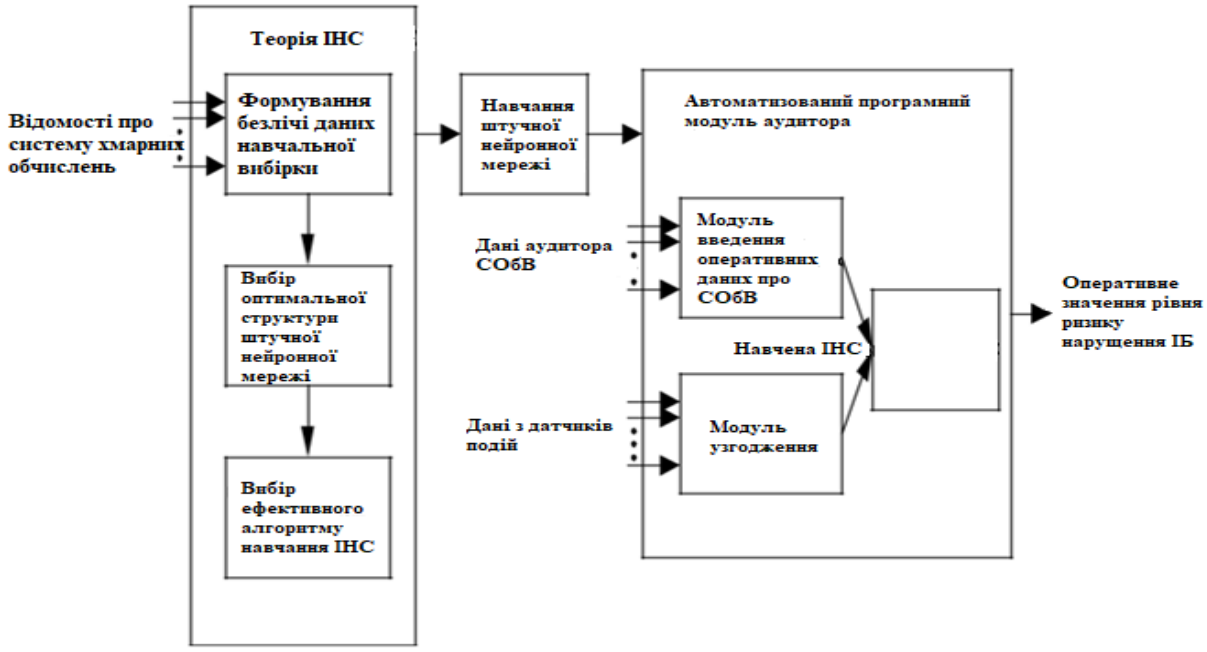

Рисунок 3.4 – Схема, що ілюструє метод проведення експертного аудиту на основі штучної нейронної мережі

Для успішного використання нейронних мереж аудитором ІБ необхідно сформувати множину даних навчальної вибірки, виходячи з поточних відомостей про розглянуту систему. Далі проводиться вибір оптимальної структури нейронної мережі та вибір ефективного за своїми параметрам алгоритму навчання ШНМ, в яких буде враховуватися специфіка навчальної вибірки. Після успішного навчання та тестування нейронної мережі на контрольних прикладах, необхідно завантажити відомості про синапси між нейронами та вагові коефіцієнти в автоматизований програмний модуль, який використовує фахівець для проведення аудиту ІБ СЗІБ.

Після навчання, ШНМ у складі системи управління ІБ забезпечить отримання оперативного значення ризику порушення інформаційної безпеки з

урахуванням актуальних даних, отриманих в процесі моніторингу інфраструктури СЗІБ датчиками подій, і даних про систему хмарних обчислень, що знаходяться в розпорядженні аудитора. На вхід навченої ШНМ подається інформація з виходу модуля введення оперативних даних про СЗІБ і з модуля узгодження даних, в якому на основі оперативних даних (отриманих з сенсорів систем виявлення вторгнень і антивірусів, з міжмережевих екранів та інших компонентів інфраструктури), виявляється джерело актуальної загрози. На виході автоматизованого програмного модуля аудитора формується оперативне значення ризику порушення ІБ.

Результати розрахунків ризиків порушення ІБ в СЗІБ при проведенні експертного аудиту можуть бути використані постачальником хмарних слуг при обговоренні зі споживачем застосованих стратегій безпеки для обґрунтування своїх можливостей щодо забезпечення захищеності критичної інформації споживача хмарних послуг і надання йому гарантованих постачальником показників. Також, оцінка ризику порушення ІБ в реальному масштабі часу дозволить здійснити вибір раціонального варіанту реагування на можливі інциденти, що виникають в системі хмарних обчислень.

Алгоритм роботи методу ШНМ представлено на рис. 3.5 [19].

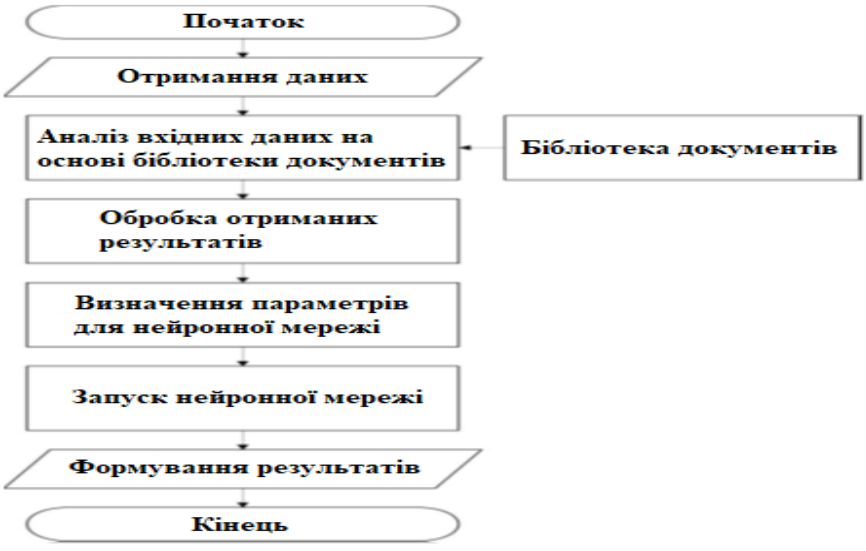

Рисунок 3.5 – Алгоритм роботи блоку штучної нейронної мережі

Функціонально програмне забезпечення складається з наступних етапів:

- перший етап формує набір дестабілізуючих факторів або здійснюється вибір з представленого списку, на основі класу автоматизованої системи;

- кожен дестабілізуючий фактор визначається ваговим коефіцієнтом;
- наступним етапом йде побудова логічних функцій і списку рішень, що приймаються. Логічні функції будуються на основі дестабілізуючих факторів. Для кожної функції задається поріг активації нейрона вхідного шару;
- на етапі, коли задаються рішення, також зі списку вибирається фактор, а потім задається поріг активації нейрона вихідного шару;
- останнім етапом служить запуск нейронної мережі і її навчання;
- навчена нейронна мережа використовується для аналізу безпеки інформаційної системи.

Чим більше вибірка данніх буде в процесі навчання, тим точніше буде прийняте рішення.

Слід зазначити, що при збільшенні числа дестабілізуючих чинників необхідно додатково проводити навчання нейронної мережі на основі вагових коефіцієнтів нових факторів. Збільшення числа дестабілізуючих факторів дозволяє розширити можливості нейронної мережі з аналізу безпеки різних інформаційних систем, при цьому варто визначати необхідний набір факторів для кожної конкретної системи.

Аналіз можливостей використання методу штучних нейронних мереж для аудиту інформаційної безпеки телекомунікаційних систем дає можливість сформулювати слідуючі висновки по використанню цього метода.

1) Для реалізації методу використовується спеціальний програмний модуль.

2) До модуля з спеціальних датчиків вводиться інформація про стан системи, що підлягає захисту. Множина цих даних використовується для навчання штучної моделі нейронної мережі.

3) Позитивною рисою методу є досить швидке обчислення стану захисту системи. Програмний модуль видає результати аудиту практично в реальному часі.

4) До недоліків методу слід віднести залежність якості результатів аудиту від кількості і правильності відбору множини даних, що входять в блок ШНМ. А це в свою чергу залежить від рівня компетентності спеціаліста з інформаційної безпеки.

4 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖ З ХМАРНИМИ ТЕХНОЛОГІЯМИ ПО РЕЗУЛЬТАТАМ АУДИТУ

Згідно з ТЗ в атестаційній роботі була поставлена задача провести аудит системи з хмарною технологією (Додаток А), виконати дослідження методів інформаційного захисту системи та розробити комплекс заходів з результатів аудиту.

На основі аналізу аудиту заданої системи можна запропонувати ряд заходів, що підвищать інформаційну безпеку системи. На рис 4.1 приведена результуюча схема системи з хмарною технологією з урахуванням заходів безпеки по результатам аудиту.

Для підвищення захисту рекомендовано.

1) Зміна апаратури точки доступ на Wi-Fi роутер з міжмережевим екраном.
2) Переміщення роутера в центр приміщення.
3) Екранування приміщення.
4) Створення захищеного тунелю по технології VPN.
5) 2-х факторний доступ співробітників до VPN каналу.

Результуюча схема системи з хмарною технологією після проведення аудиту зображена на рис. 4.1.

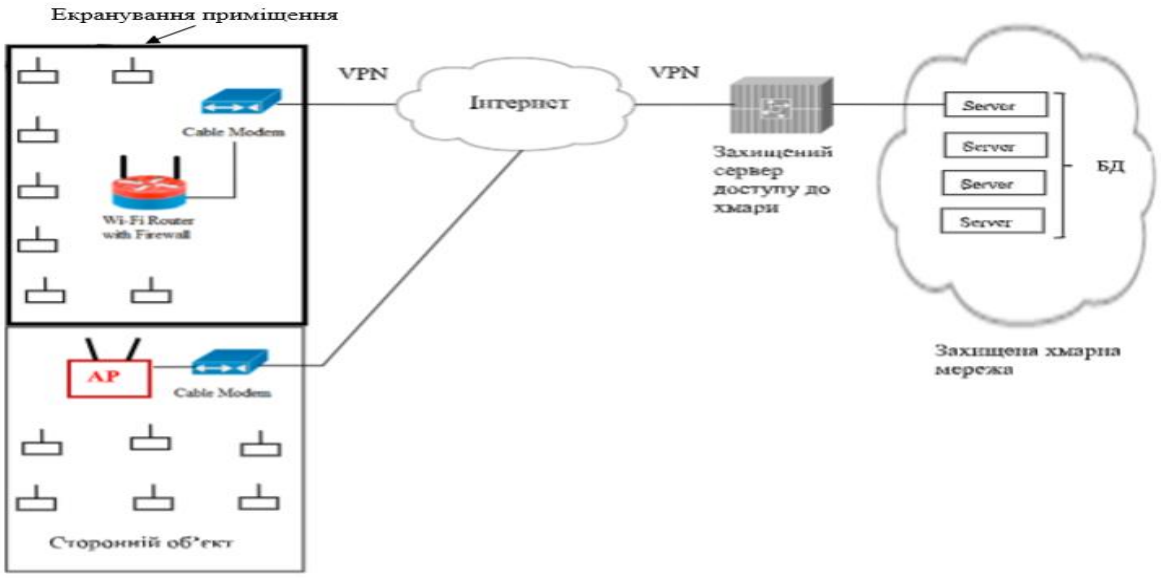

Рисунок 4.1 – Результуюча схема системи з хмарною технологією з заходами інформаційної безпеки по результатам аудиту

Для перевірки запропонованих методів дули проаналізовані додаткові організаційні заходи з урахуванням специфіки хмарної технології, а також проведені реальні експериментальні дослідження аналогічних ситуацій на фізичному рівні з дослідженням розподілення електромагнітних полів джерелл радіо випромінювання. Крім цього проведено реальне експериментальне дослідження по створенню захищеного каналу з використанням технології VPN.

Результати цих досліджень наведені в наступних підрозділах атестаційної роботи.

4.1 Організаційні заходи

Організаційні заходи для мережі з використанням хмарної технології традиційні з додаванням заходів, що викликані необхідністю взаємодії з хмарою.

Потрібно виділити особливи критичні види інформації, що не можуть бути розміщені в хмарі.

З великою обережністю треба вибирати постачальника хмарних послуг, який користується довірою замовника послуг.

Особливу увагу приділити портам, що з’єднують мережу фірми з хмарою. Вони повинні бути захищеними з використанням усіх можливих засобів.

4.2 Заходи на фізичному рівні

Потрібно провести аудит фізичного середовища, якщо в фірмі є безпровідний сегмент. Це потрібно зробити за допомогою спеціальних засобів обстеження територіії на розподілення електромагнітного поля і наявність усіх точок доступу.

Виробити рекомендації по розміщенню штатних точок доступу фірми і робочих місць з рекомендованою зоною їх дії, що зменшує можливість прослуховування.

Можливо ввести додаткові засоби, наприклад, екранування приміщень, або покриття стін поглинаючими шарами спеціальних матеріалів.

Було проведено експеримент аудиту двох приміщень. Перший результат получено за допомогою програми Ekahau Heat Mapper рис. 4.2, а другий за допомогою програми TamoGraph рис. 4.3. Програма TamoGraph більш

функціональна, але є платною. В експерименті використана демо версія програми з урізаними можливостями.

Зелений колір велика потужність, від жовтого до червоного – зменшення потужности поля.

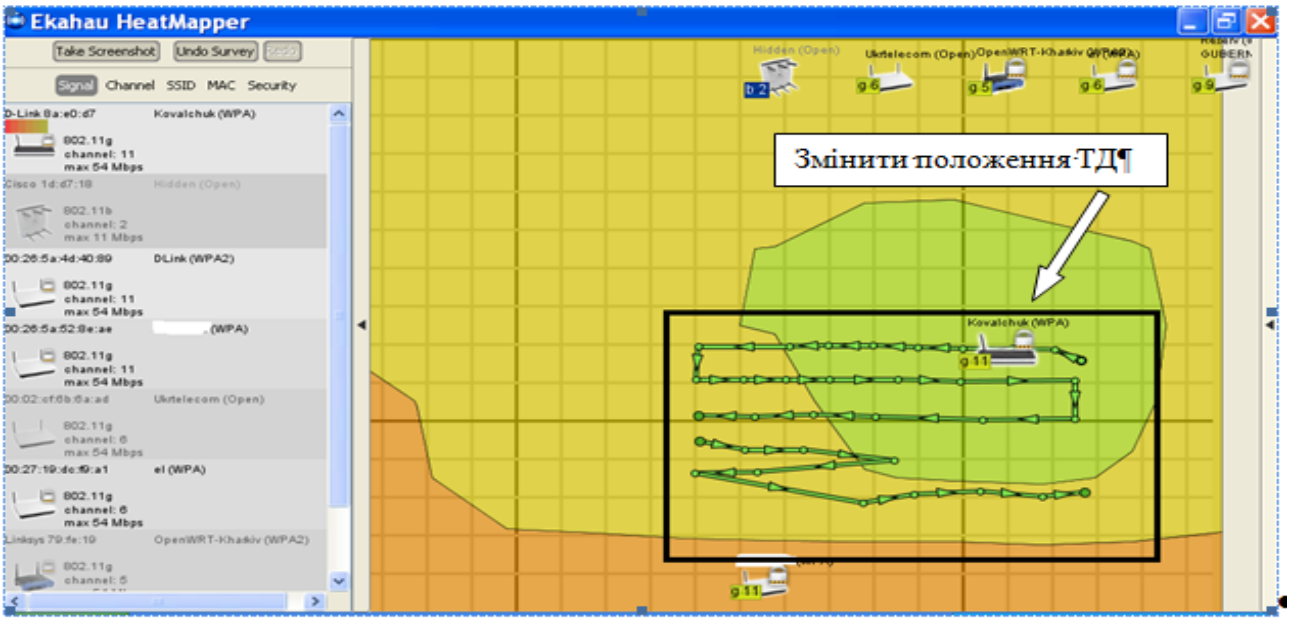

Рисунок 4.2 – Результат аудиту приміщення № 1 за допомогою програми Ekahau Heat Mapper

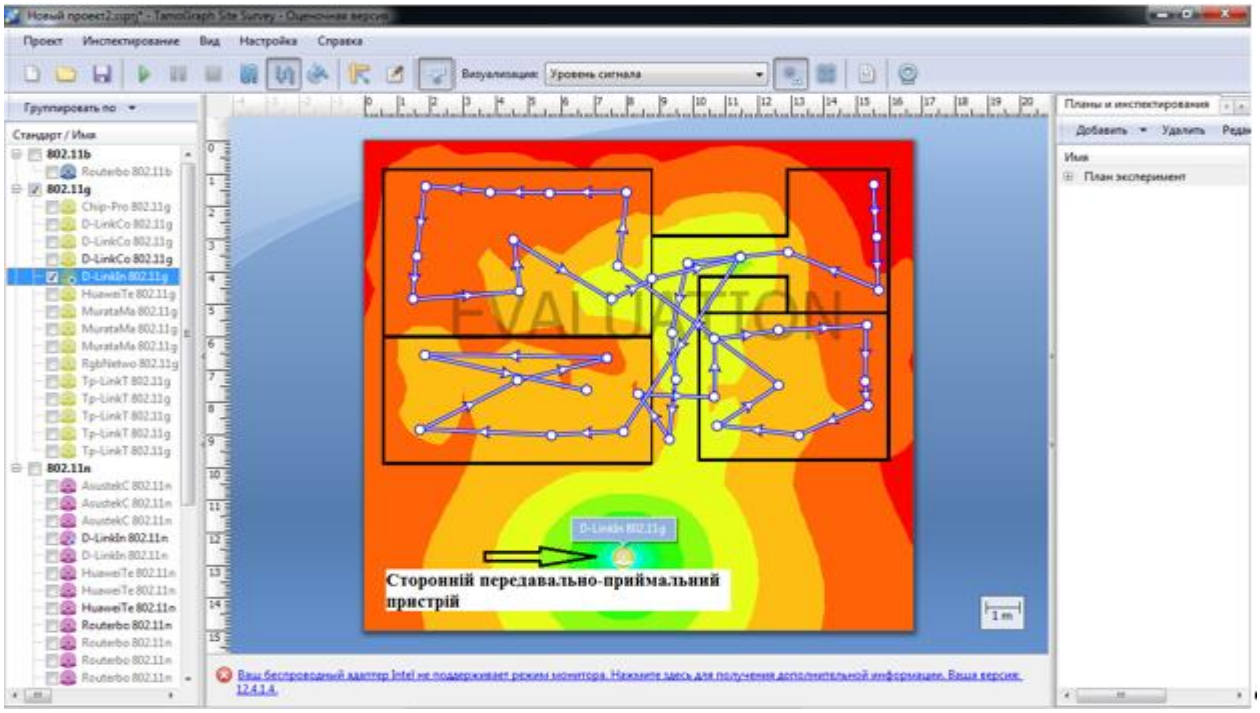

Рисунок 4.3 – Результат аудиту приміщення № 2 за допомогою програми TamoGraph (демо)

По результатам експериментів аудиту приміщень можна запропонувати слідуючі заходи безпеки. По першому приміщенню рекомендується змінити положення точки доступу. Треба її розмістити в середині об’єкту подалі від стін.

По другому приміщенню потрібно зробити екранування приміщення і доповнити його покриттям стін поглинаючим радіохвилі шаром. Це дозволить на фізичному рівні захиститися від стороннього джерела.

4.3 Заходи на програмному рівні

По результатам аудиту телекомунікаційної системи з хмарною технологією пропонується ввести в неї систему виявлення і запобігання вторгнень IDS та IPS.

Всі існуючі сьогодні системи виявлення та запобігання вторгнень об'єднані кількома загальними властивостями, функціями і завданнями, які з їх допомогою вирішують фахівці з інформаційної безпеки. Такі інструменти здійснюють безперервний аналіз експлуатації ресурсів мережі і виявляють будь-які ознаки нетипових подій.

Організація безпеки мереж може бути основана на декількох технологіях, які відрізняються типами виявлених інцидентів і методами, що застосовуються для виявлення таких подій. Крім функцій постійного моніторингу та аналізу того, що відбувається, всі IDS системи виконують такі функції:

- збір і запис інформації;
- оповіщення адміністраторів мереж про зміни, що відбулися в системі;
- створення звітів для підсумовування логів.

Технологія IPS в свою чергу доповнює IDS, так як здатна не тільки визначити загрозу і її джерело як IDS, а й здійснити блокування загрози. IPS здатна здійснювати наступні дії:

- обривати шкідливі сесії і запобігати доступ до найважливіших ресурсів;
- змінювати конфігурацію «підзахисного» середовища;
- проводити дії над інструментами атаки (наприклад, видаляти заражені файли).

Технологія IPS використовує методи, засновані на сигнатурах - шаблонах, з якими пов'язують відповідні інциденти. У якості сигнатур можуть бути різні з’єднання системи з зовнішніми абонентами, електронні листи, логи операційної

системи і т.п. Такий спосіб детекції вкрай ефективний при роботі з відомими погрозами, але дуже слабкий при атаках, які не мають сигнатур.

Можна рекомендувати ще один метод виявлення несанкціонованого доступу HIPS. Метод HIPS полягає в статистичному порівнянні рівня активності подій з нормальним, значення якого були отримані під час так званого «навчального періоду». Засіб виявлення вторгнень може доповнювати сигнатурну фільтрацію і блокувати хакерські атаки, які змогли її обійти.

Одним з рішень IPS для запобігання вторгнень є детектори атак, які призначені для своєчасного виявлення множини шкідливих загроз. Робота детектора атак заснована на аналізі сигнатур і евристиці.

Обов’язково рекомендується також в телекомунікаційній мережі з хмарною технологією використовувати антивірусний захист з постійним його оновленням.

Новий напрямок в технологіях захисту – це використання хмарних антивірусних систем. Цей метод має як позитивні, так і негативні якості.

4.4 Використання технології тунелювання Virtual Private Network

По результатам аудиту основним каналом, що піддається атакам в системах з хмарною технологією є канал зв’язку до хмари і в зворотньому напрямку. Тому, що це вихід в зовнішнє середовище за межі захищеного об’єкта.

Для реалізації захищеного каналу до хмари запропоновано використати технологію VPN. В даний час поширені три види організації VPN на мережевому рівні.

1) Point-to-point tunnel protocol (PPTP).
2) IPSec-ESP в тунельному режимі.
3) Layer 2 Tunnel Protocol (L2TP) спільно з IPSec-ESP.

Протокол IPSec підтримує два режими роботи: транспортний і тунельний. У транспортному режимі вихідний заголовок IP практично не змінюється. Тунельний режим має на увазі захист всього вихідного пакета і додавання нового IP-заголовка, можливо, з іншими адресами відправника і одержувача. Таким чином, транспортний режим використовується для захисту взаємодії між вузлами, а тунельний - між двома мережами або вузлом і мережею.

Для нашого випадку доцільно використання більш захищеного тунельного режиму.

В середині об’єкта є відділ з безпровідною технологією IEEE 802.11. Для зв’язку з хмарою потрібно мати захищений канал.

Проведемо експериментальне дослідження можливості організації VPN тунелю.

Експериментальна установка складається з ПК з ОС Windows, встановленим ПЗ Oracle VirtualBox, що має вихід в Інтернет і точки доступу стандарту IEEE 802.11g до якої підключається інші ПК безпровідної мережі. Схема експеременту по створенню VPN тунелю до хмари зображена на рис. 4.4.

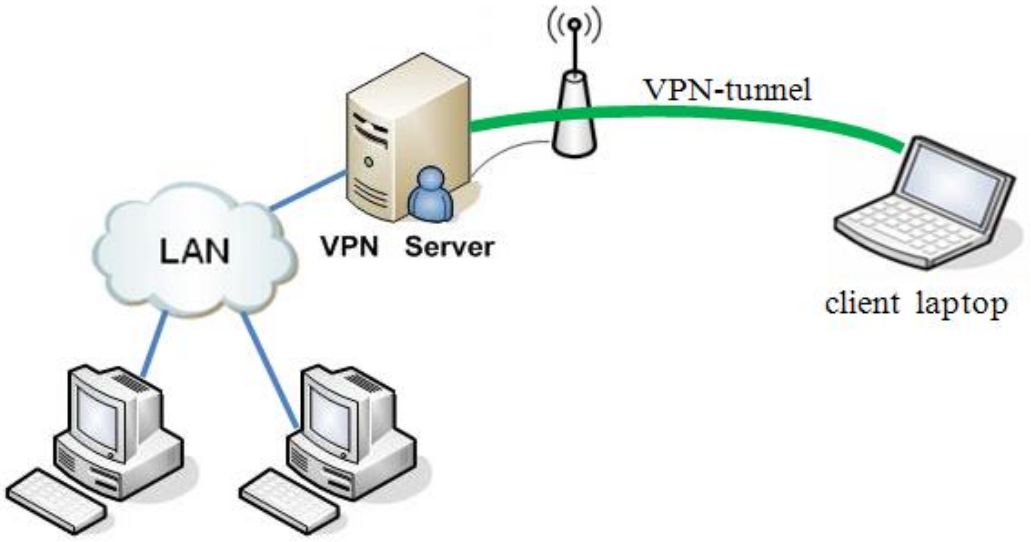

Рисунок 4.4 – Схема експерименту по створенню VPN тунелю до хмари

У VPN-тунелі будемо використовувати шифрування трафіку. Це дозволить здійснювати безпечний доступ до корпоративних ресурсів компанії. Також за допомогою аутентифікації на сервері VPN і відповідних правил фільтрації пакетів на шлюзі, буде розділений гостьовий доступ до Інтернету і доступ співробітників фірми до корпоративних ресурсів.

Завантажуємо ОС Ubuntu. Коли ОС завантажиться, перевіряємо, що комп'ютер отримав IP адресу по протоколу DHCP і що у нього є зв'язок з Інтернет.

Відкриваємо діалогове вікно оновлень ПЗ «Software & Updates». Данне вікно зображено на рис. 4.5.

Рисунок 4.5 – Діалогове вікно оновлень програмного забезпечення "Software & Updates"

Ставимо галочку для підключення репозиторію universe. Він знадобиться при завантаженні та інсталяції деяких необхідних нам пакетів, приклад даного вікна зображений на рис 4.6.

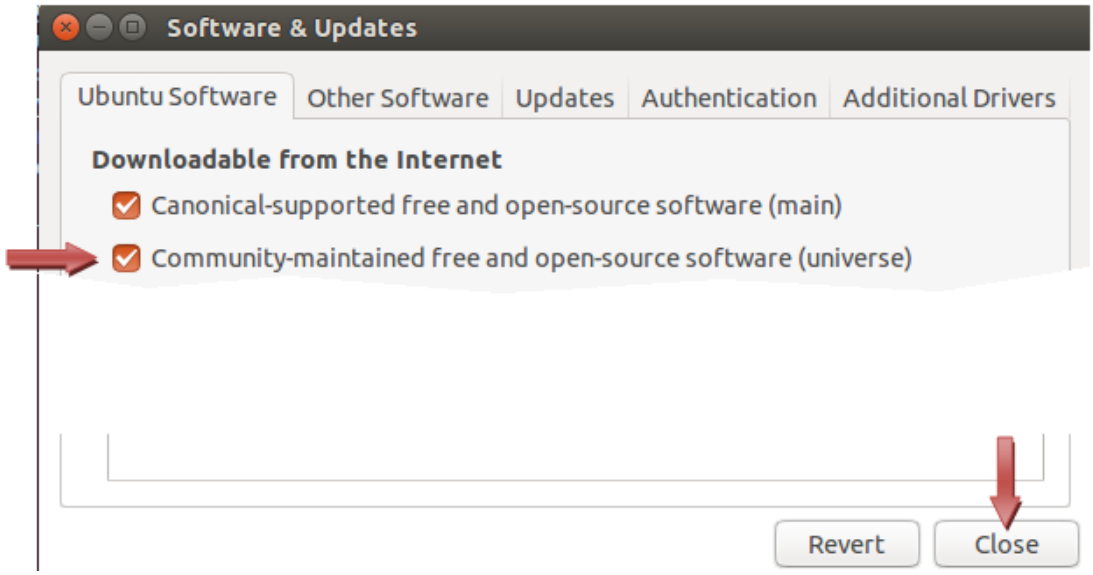

Рисунок 4.6 – Вікно підключення репозиторію universe

Встановлюємо час і часовий пояс такий же як і у клієнта (Київський час), щоб не виникло проблем при перевірці сертифікатів. Для цього клацаємо мишкою у верхньому правому куті, там де годинник і вибираємо «Date & Time Settings».

Встановлюємо додаткове ПЗ. Запускаємо термінал «Ctrl + Alt + T» і переходимо в режим суперкористувача «sudo su».

Встановлюємо пакети «apt-get install»для цього потрібно виконати наступні етапи.

1) Apt-get install easy-rsa.
2) Apt-get install openvpn.
3) Apt-get install mc.

Запускаємо Midnight Commander (набираємо «mc»), копіюємо директорію «easy-rsa», яка знаходиться в директорії «/usr/share/» так, щоб вона перебувала в «/etc/openvpn/easy-rsa/».

Редагуємо файл «/etc/openvpn/easy-rsa/vars» згідно з даними, які будуть відображатися в сертифікатах для VPN:

- export KEY_COUNTRY=”UA”;
- export KEY_PROVINCE=”Kharkiv”;
- export KEY_CITY=” Kharkiv”;
- export KEY_ORG=”ICI”;
- export KEY_EMAIL=”tkc@nure.ua”;
- export KEY_CN=MyVPN;
- export KEY_NAME=MyVPN;
- export KEY_OU=MyVPN.

Створюємо директорію «keys» так щоб вона була в «/ etc / openvpn / easy-rsa / keys», далі робимо такі дії.

1) Переходимо в директорію «/ etc / openvpn / easy-rsa/».
2) Натискаємо «Ctrl + O» щоб переключитися в консоль.
3) Виділяємо команду для установки вихідних значень змінних, які будуть використовуватися в скриптах «source./vars».
4) Виділяємо команду для очищення директорії «keys./clean-all».
5) Створюємо кореневий сертифікат ca для центру сертифікації CA «./build-ca».
6) Створюємо сертифікат для сервера. Він буде використовуватися при створенні «./build-key-server your server name».
7) Приймаємо всі значення за замовчуванням (вони задані у файлі «vars»), крім пароля.
8) Набераємо «yes» для того щоб підписати і зберегти в базі сертифікат.
9) Необхідно також згенерувати параметр «Diffie Hellman», набираємо «./bulid-dh».

10) Тепер генеруємо сертифікат клієнта. Після генерації їх потрібно буде передати клієнту «./build-key your_client_name».

11) Прінімаємо всі значення за замовчуванням (вони задані у файлі «vars»), крім пароля.

12) Набераємо «y» для того щоб підписати і зберегти в базі сертифікат.

13) Генеруємо TLS-auth ключ «openvpn --genkey --secret ta.key», за замовчуванням він з'являється в «/etc / openvpn/».

14) Потім зберігаємо на флешку наступні файли для клієнтської сторони: «/etc/openvpn/ca.crt», «/etc/openvpn/easy-rsa/keys/your_client_name.crt», «/etc/open vpn /easy-rsa/keys/your_client_name.key», «/etc/openvpn/ta.key».

15) Далі виконуємо конфігурування і запуск OpenVPN.

Існує приклад початкової конфігурації OpenVPN сервера який заархівований і зберігається за адресою «/usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz».

Розкриваємо архів і поміщаємо його за адресою «/etc/openvpn /», це можна зробити з командного рядка за допомогою команди «zcat».

Щоб не писати довгий шлях до першого файлу переходимо в директорію «sample-config-files» і набираємо відносний шлях «zcat ./server.conf.gz > «/etc/openvpn/server.conf», коли з'явиться файл «server.conf» внесемо в нього зміни, конфігурація налаштування наведена в додатку Б. Після збереження конфігурації, запускаємо OpenVPN за допомогою команди «service openvpn start».

На останньому етапі виконуємо конфігурування OpenVPN клієнта.

Переходимо в директорію «/usr/share/doc/openvpn/examples/sample-config-files» і копіюємо на флешку файл «client.conf». Він містить приклад налаштувань VPN клієнта, данний файл детальніше можна роздивитися в додатку В.

Особливу увагу потрібно звернути на такі настройки – IP адреса VPN (в конфігурації клієнта це рядок «remote»). Він повинен збігатися з його адресою (це можна побачити в консолі на Ubuntu ввівши команду «ifconfig»). Також назви файлів з сертифікатами і ключами повинні відповідати їх реальним назвам.

Проводимо налаштування OpenVPN клієнта для Windows 7.

Перейменовуємо конфігураційний файл «client.conf» в «client.ovpn». Тобто для Windows цей файл повинен мати розширення «.ovpn».

Запускаємо інсталятор OpenVPN, початок установки програми на рис. 4.7 та підтвердження установки драйвера на рис. 4.8.

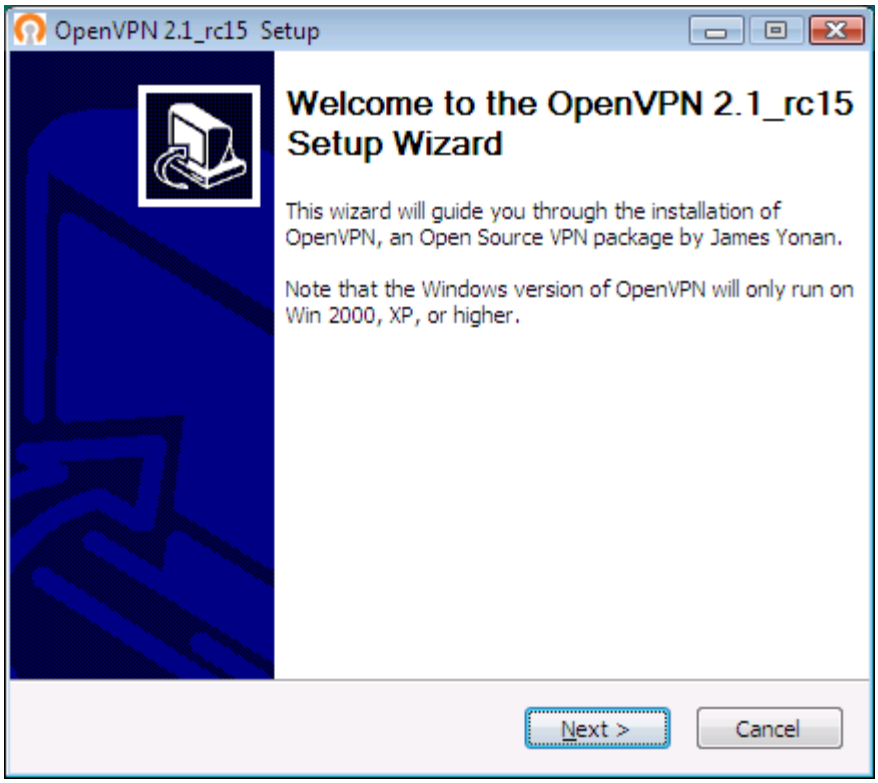

Рисунок 4.7 – Початок установки програми

Рисунок 4.8 – Підтвердження установки драйвера

Установка проходить без будь-яких складнощів. Досить натискати кнопку «Next» - «Далі». На запит про встановлення драйвера відповідаємо позитивно- «Install» - «Встановити».

Після установки, відкриваємо каталог в якому знаходяться конфігураційні файли програми через «Головне меню»: «Start-All Programs-OpenVPN-Shortcuts-OpenVPN configuration file directory», каталог для файлів налаштування можна подивитися на рис. 4.9.

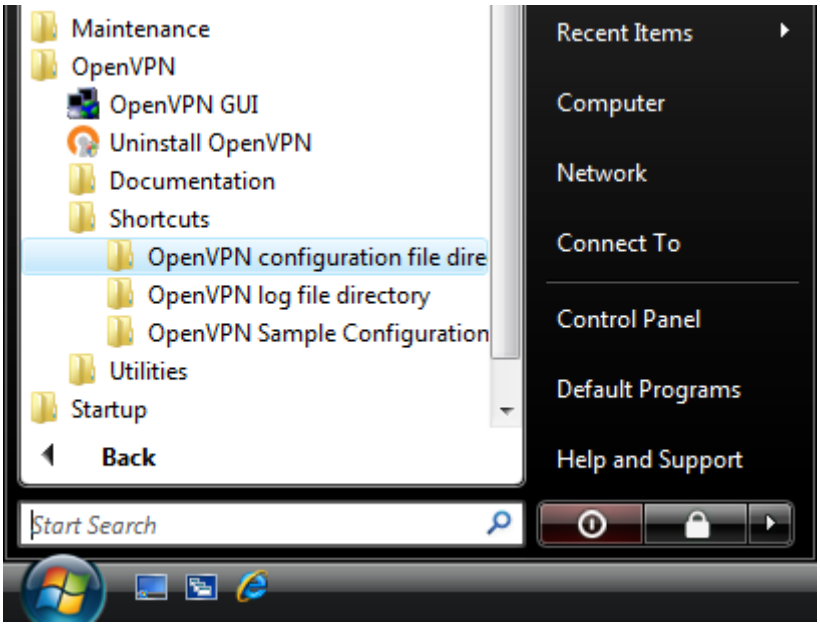

Рисунок 4.9 – Каталог для файлів налаштування

Копіюємо в цей каталог файли, що збережені на флешці. На рис. 4.10 зображено копіювання ключів і конфігураційних файлів.

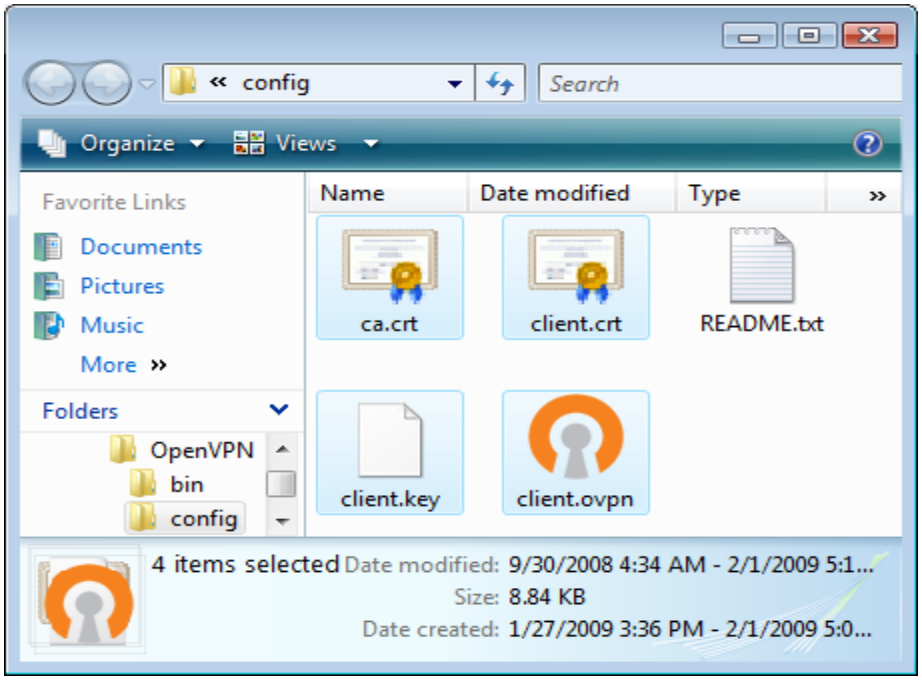

Рисунок 4.10 – Копіювання ключів і конфігураційних файлів

Після копіювання файлів відкриваємо контекстне меню ярлика OpenVPN (права клавіша миші). Запускаємо програму від імені адміністратора. Потім налаштовуємо параметри для коректного запуску, налаштування зображено на рис. 4.11.

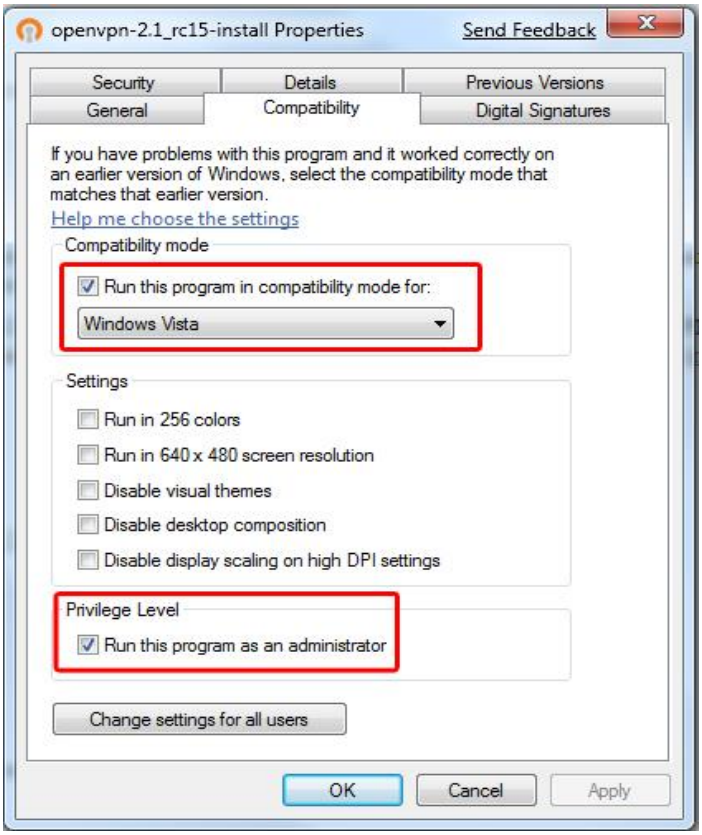

Рисунок 4.11 – Налаштування параметрів для коректного запуску

Для перевірки працездатності VPN спочатку підключаємо клієнта до сервера, приклад наведено на рис. 4.12. Потім запускаємо програму OpenVPN GUI. На панелі задач побачимо результат «Connect» і «client is now connected».

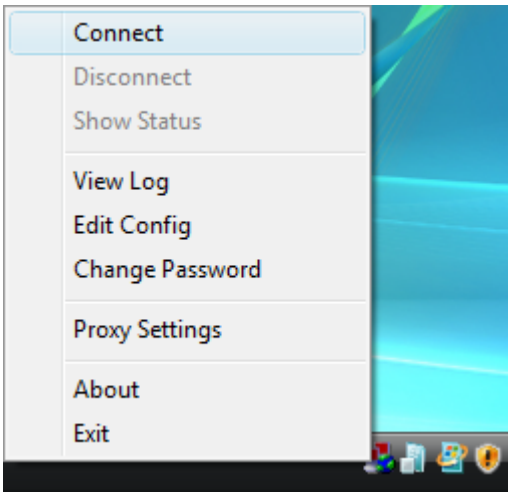

Рисунок 4.12 – Підключення

Після успішного підключення до сервісу у спливаючому вікні з'являється інформація про з'єднання рис. 4.13.

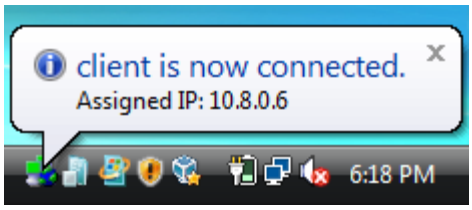

Рисунок 4.13 – Інформація про успішне підключення

4.5 Використання шлюзів захисту Firewall

Firewall є пристроями, які керують потоком мережевого трафіку між мережами з різними вимогами до безпеки. У більшості сучасних додатків вони використовуються для з'єднань в Інтернеті і, отже, використання стека протоколів TCP/IP.

Сучасні Firewall функціонують майже на всіх рівнях моделі OSI. З точки зору функціональності Firewall, що має можливість аналізувати більше число рівнів, є більш досконалим і ефективним. За рахунок охоплення додаткового рівня також збільшується можливість більш тонкої настройки його конфігурації. Можливість аналізувати більш високі рівні дозволяє Firewall надавати сервіси, які орієнтовані на користувача, наприклад, аутентифікація користувача.

Незалежно від архітектури Firewall може мати додаткові сервіси. Ці сервіси включають трансляцію мережевих адрес NAT, підтримку протоколу динамічної конфігурації хоста DHCP і функції шифрування, тим самим будучи кінцевою точкою VPN-шлюзу, і фільтрацію на рівні вмісту програми.

Проксі прикладного рівня є більш потужними Firewall, які комбінують управління доступом на низькому рівні з функціональністю більш високого рівня (Рівень 7 – Application), саме на рис. 4.14 показано перелік трафиків, що можуть управлятися прокси Firewall.

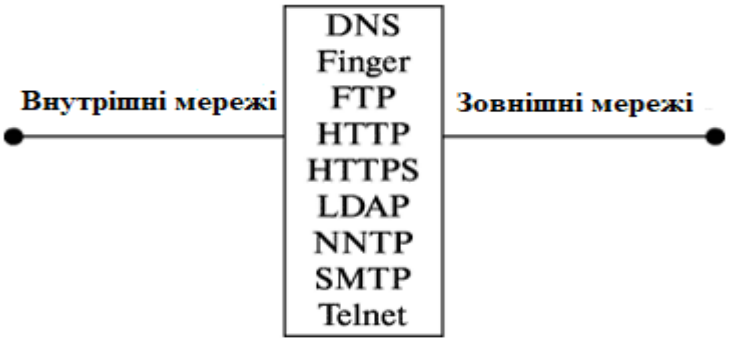

Рисунок 4.14 – Проксі Firewall з управлінням множиною трафиків

Окрім системи Firewall можна ввести в систему, що підлягає захисту досить простий фільтр – утиліту ip table.

С точки зору використання ip table трафік буває 3-х типів:

- вхідний;
- транзитний;
- вихідний.

Всі пакети приходять на мережеву карту проходять всі 7 рівнів моделі OSI. Ip tables починає обробку пакетів з 3-го (мережевого) рівня.

Після того як пакет з лінії зв'язку потрапив на мережеву карту, він передається в ядро операційної системи (ОС), а саме в netfilter. Далі пакет проходить ряд таблиць і тільки після цього потрапляє в додаток (або не потрапляє, якщо пакет йшов транзитом), якому він був адресований. Саме таблицями і правилами ядра netfilter управляє утиліта ip table.

Для всіх видів трафіку можна запрограмувати політики роботи: які пакети пропускати, які блокувати, як в одну, так і в зворотний бік (з нашої мережі і в нашу мережу). При цьому можна записати таблицю IP адрес дозволених і заборонених.

Ip table має ще одне важливе застосування. Цей програмний продукт дозволяє виконувати маскування мережі.

Маскування таким чином, що кілька машин з внутрішньої мережі можуть звертатися до зовнішньої мережі, а ззовні це буде виглядати так, як ніби звернення йдуть від машини, що є шлюзом. А функцію шлюзу виконує ip table.

Маскарадінг пов'язаний в першу чергу з NAT, пакети при трансляції адрес маскуються (замінюються), щоб відповідь повернувся саме до джерела запиту.

ВИСНОВКИ

Аудит інформаційної безпеки на сьогоднішній день є одним з найбільш ефективних інструментів для отримання незалежної і об'єктивної оцінки поточного рівня захищеності підприємства від загроз інформаційної безпеки. Крім того, результати аудиту є основою для формування стратегії розвитку системи забезпечення інформаційної безпеки організації. Однак, необхідно пам’ятати, що аудит безпеки мережі не є одноразовою процедурою, а повинен проводитися на регулярній основі. Тільки в цьому випадку аудит буде приносити реальну користь і сприяти підвищенню рівня інформаційної безпеки компанії.

Програма аудиту та забезпечення достовірності повинна періодично перевіряти конфігурацію системи і стан інформаційної безпеки, щоб уникнути кібератак. Хмарні технології є важливим компонентом в організації, тому важливо, щоб ця система була забезпечена міцним захистом від витоку важливої інформації. Саме на це спрямована головна мета цієї атестаційної роботи.

Отже для забезпечення захисту хмарних технологій слід враховувати усі фактори, які можуть порушити доступність, цілісність або конфіденційність інформації. Також, дуже важливим правилом є те, що покращення безпеки однієї з властивостей не повинно загрожувати зменшенню чи втраті інших, тобто всі методи запобігання загрозам мають взаємодіяти у балансі, захищаючи дані та інформацію з усіх кутів.

У даній атестаційній роботі на тему: «Аналіз інформаційної безпеки телекомунікаційної мережі з хмарною технологією», було досліджено саме поняття аудиту, були виокремлені компоненти аудиту інформаційної безпеки, виявлені важливі фактори та причини, з яких потрібно розгортати аудит інформаційної безпеки мережі організації, було оцінено цінність та важливість аудиту для бізнесу, було розглянуто аудит інформаційної безпеки телекомунікаційних мереж з хмарною технологією з використанням методу на основі штучної нейронної мережі та розроблений метод та структурна схема, що реалізує метод проведення експертного аудиту інформаційної безпеки в системі хмарних обчислень, також були досліджені методи захисту мереж з хмарними технологіями по результатам аудиту.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Корпоративна мережа [Електронний ресурс].– 2017. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Корпоративна_мережа.

2. Аудит інформаційної безпеки – основа ефективного захисту підприємства [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.intuit.ru/studies/courses/600/456/lecture/10226.

3. Скирда С. О. Аудит інформаційної безпеки телекомунікаційних мереж з хмарною технологією / С. О. Скирда, А. М. Стрілець, В. Г. Чернікова // Матеріали 24-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь в XXI столітті». – Харків: ХНУРЕ, 2020 – С. 227-228.

4. Загрози інформаційної безпеки [Електронний ресурс].– 2017. – Режим доступу до ресурсу: http://www.internet-technologies.ru/articles/article_1147.html.

5. Інтернет-Університет Інформаційних Технологій [Електронний ресурс].– 2015. – Режим доступу до ресурсу: http://www.intuit.ru/department/security/secbasics/1/secbasics_1.html.

6. Хмарні обчислення-переваги і недоліки [Електронний ресурс].– 2015. – Режим доступу до ресурсу: http://www.smart-cloud.org/sorted-articles/44-for-all/96-cloud-computing-plus-minus.

7. Безпека хмарних обчислень [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: http://www.pcmag.ru/solutions/detail.php?ID=38248.

8. Основи хмарних технологій [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://www.stgau.ru/company/personal/user/7684/files/lib.

9. John Dinsdeil SynergyResearch Group [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: synergycro.ru.

10. Авраменко А. П. «Хмарні обчислення» / А. П. Авраменко // JetInfo. No 10, 2010. З. 63-75.

11. CISA Exam Preparation Course [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.udemy.com.

12. What is CRAMM? [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: http://www.gammassl.co.uk/topics/hot5.html

13. SANS/GIAC Site Certification Program [Електронний ресурс]. – 2008. – Режим доступу до ресурсу: http://www.sans.org/SCORE.

14. SysTrust Services Program [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: http://www.aicpa.org/assurance/systrust/index.htm.

15. Перегудов Ф. І. Введення в системний аналіз: Учеб. Посібник для вузів / Ф.І. Перегудов, Ф. П. Тарасенко. – М. : Вища школа, 1989. – 367 с.

16. Шумський А. А.Сістемний аналіз в захисті інформації: навч. Посібник для студентів вузів, які навчаються за спеціальностями в обл. ІБ / А. А. Шумський, А. А. Шелупанов. – М. : Геліос АРВ, 2005. – 224 с.

17. Перегудов Ф. І. Введення в системний аналіз: Учеб. Посібник для вузів / Ф. І. Перегудов, Ф. П. Тарасенко. – М. : Вища школа, 1989. – 367 с.

18. Гузаіров М. Б. Метод визначення цінності інформації з використанням апарату нечіткої логіки / М. Б. Гузаіров, І. В. Машкіна, Е. С. Степанова // Безпека інформаційних технологій. No1, 2012. З 18-29.

19. Е. В. Трапезников. Реализация модели анализа защиты информации на основе нейронной сети// Динамика систем, механизмов и машин. 2017. Том 5, № 4. С.105-110.

20. Стрілець А. М. Методи тестування засобів захисту інформації / А. М. Стрілець, С. О. Скирда, В. Г. Чернікова // Матеріали 24-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь в XXI столітті». – Харків: ХНУРЕ, 2020 – С. 217-218.

21. Чернікова В. Г. Дослідження методів захисту біометричного шаблону райдужної оболонки ока / В. Г. Чернікова, С. О. Скирда, А. М. Стрілець // Матеріали 24-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь в XXI столітті». – Харків: ХНУРЕ, 2020 – С. 179-180.

22. Скирда С. О. Аналіз вразливостей Windows – подібних серверних операційних систем та загальне описання механізмів їх захисту / С. О. Скирда // Міжнародна науково-практична конференції «Інформаційна безпека та інформаційні технології», 24-25 квітня 2019 року, м. Харків, ХНЕУ ім. С. Кузнеця. 2019. – 20 с.